CA Network Flow Analysis

Manuel de mise à niveau

Version 9.3.0



Support technique

Pour une assistance technique en ligne et une liste complète des sites, horaires d'ouverture et numéros de téléphone, contactez le support technique à l'adresse http://www.ca.com/worldwide.

Documentation connexe

CA fournit une documentation technique complète dans la bibliothèque de CA Network Flow Analysis. Accédez à la bibliothèque en cliquant sur le lien Aide dans l'interface utilisateur de CA Network Flow Analysis. Les fichiers PDF et HTML des manuels sont disponibles dans la bibliothèque de la documentation.

La documentation a peut-être été mise à jour depuis sa publication. Pour connaître les dernières mises à jour de la documentation CA Network Flow Analysis et obtenir les versions localisées de la documentation, téléchargez la bibliothèque à partir du site de support CA.

La documentation de CA Network Flow Analysis 9.3.0 inclut les manuels suivants :

- *Aide en ligne* : assistance destinée aux administrateurs et opérateurs, disponible à partir du lien Aide dans l'interface utilisateur
- *Manuel de l'administrateur* : procédure de configuration et de maintenance de CA Network Flow Analysis
- *Manuel de l'opérateur* : procédure d'utilisation de la console NFA pour la création, l'affichage et la gestion des rapports
- *Manuel d'installation* : procédure d'installation du logiciel et de réalisation des tâches de configuration à usage unique
- *Manuel de mise à niveau* : procédure de mise à niveau du logiciel et de réalisation des tâches initiales de configuration
- *Notes de parution* : récapitulatif des améliorations apportées à CA Network Flow Analysis, des corrections et des problèmes en cours de résolution
- *Manuel de CA Anomaly Detector* : procédure d'installation, de mise à niveau, de configuration et d'utilisation de CA Anomaly Detector
- *Notes de parution de CA Anomaly Detector* : présentation du produit, configuration/recommandations système requises et fonctionnalités

Les PDF du produit se trouvent dans le répertoire suivant : <chemin_installation>\Reporter\NetQoS.ReporterAnalyzer.WebSite\help\fr_FR\NFA_Bookshelf\Bookshelf_Files\PDF.

Adobe Reader doit être installé pour pouvoir afficher les fichiers de documentation au format PDF.

Table des matières

Chapitre 1: Introduction

Ce manuel décrit la procédure de mise à niveau vers CA Network Flow Analysis 9.3.0.

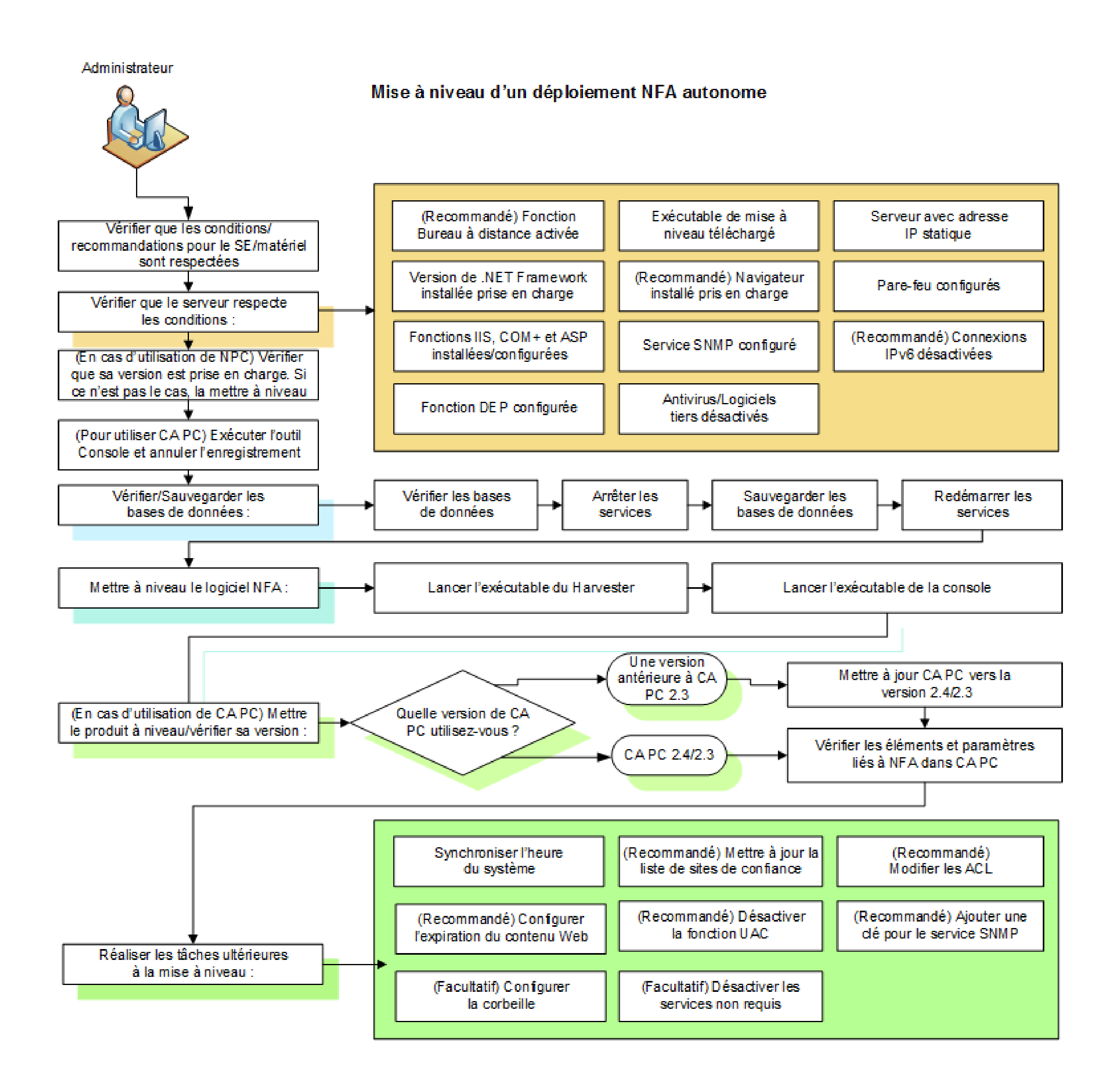
Si vous achetez du matériel auprès de CA Technologies, tous les composants sont livrés avec le système d'exploitation et les paramètres de sécurité déjà configurés. Utilisez les rubriques de ce manuel pour vérifier les paramètres ou pour les mettre à jour suivant les besoins de votre organisation.

Si vous achetez des logiciels uniquement, configurez et sécurisez le système d'exploitation suivant les descriptions contenues dans cette section.

Les diagrammes suivants affichent les étapes nécessaires à la mise à niveau de CA Network Flow Analysis.

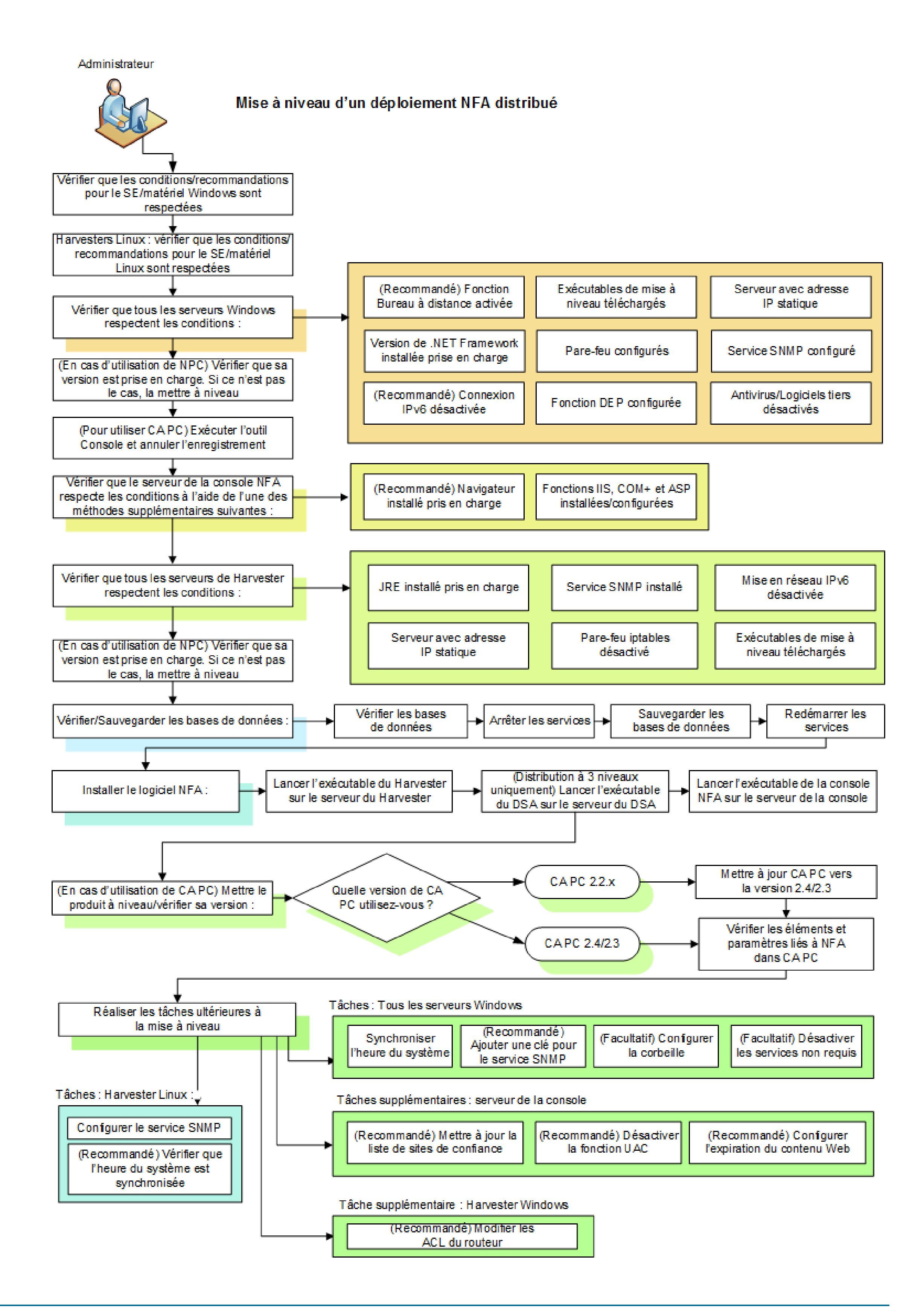
Flux de travaux pour la mise à niveau du produit dans un déploiement autonome

Utilisez le diagramme suivant comme liste de contrôle générale pour la mise à niveau d'un déploiement autonome. Pour des informations complètes concernant les étapes, reportez-vous aux rubriques associées.



Flux de travaux pour la mise à niveau du produit dans un déploiement distribué

Utilisez le diagramme suivant comme liste de contrôle générale pour la mise à niveau d'un déploiement distribué. Pour des informations complètes concernant les étapes, reportez-vous aux rubriques associées.



Administrateur
Mise à niveau d'un déploiement NFA distribué
Vérifier que les conditions/recommandations pour le SE/matériel Windows sont respectées
Harvesters Linux : vérifier que les conditions/ recommandations pour le SE/matériel Linux sont respectées
Vérifier que tous les serveurs Windows respectent les conditions :
(Recommandé) Fonction Bureau à distance activée
Exécutables de mise à niveau téléchargés
Serveur avec adresse IP statique
Version de .NET Framework installée prise en charge
Pare-feu configurés
Service SNMP configuré
(Recommandé) Connexion IPv6 désactivée
Fonction DEP configurée
Antivirus/Logiciels tiers désactivés
(En cas d'utilisation de NPC) Vérifier que sa version est prise en charge. Si ce n'est pas le cas, la mettre à niveau
(Pour utiliser CA PC) Exécuter l'outil Console et annuler l'enregistrement
Vérifier que le serveur de la console NFA respecte les conditions à l'aide de l'une des méthodes supplémentaires suivantes :
(Recommandé) Navigateur installé pris en charge
Fonctions IIS, COM+ et ASP installées/configurées
Vérifier que tous les serveurs de Harvester respectent les conditions :
JRE installé pris en charge
Service SNMP installé
Mise en réseau IPv6 désactivée
Serveur avec adresse IP statique
Pare-feu iptables désactivé
Exécutables de mise à niveau téléchargés
(En cas d'utilisation de NPC) Vérifier que sa version est prise en charge. Si ce n'est pas le cas, la mettre à niveau
Vérifier/Sauvegarder les bases de données :
Vérifier les bases de données
Arrêter les services
Sauvegarder les bases de données
Redémarrer les services
Installer le logiciel NFA :
Lancer l'exécutable du Harvester sur le serveur du Harvester
(Distribution à 3 niveaux uniquement) Lancer l'exécutable du DSA sur le serveur du DSA
Lancer l'exécutable de la console NFA sur le serveur de la console
(En cas d'utilisation de CA PC) Mettre le produit à niveau/vérifier sa version :
Quelle version de CA PC utilisez-vous ?
CA PC 2.2.x
Mettre à jour CA PC vers la version 2.4/2.3
CA PC 2.4/2.3
Vérifier les éléments et paramètres liés à NFA dans CA PC
Réaliser les tâches ultérieures à la mise à niveau
Tâches : Tous les serveurs Windows
Synchroniser l'heure du système
(Recommandé) Ajouter une clé pour le service SNMP
(Facultatif) Configurer la corbeille
(Facultatif) Désactiver les services non requis
Tâches : Harvester Linux :
Configurer le service SNMP
(Recommandé) Vérifier que l'heure du système est synchronisée
Tâches supplémentaires : serveur de la console
(Recommandé) Mettre à jour la liste de sites de confiance
(Recommandé) Désactiver la fonction UAC
(Recommandé) Configurer l'expiration du contenu Web
Tâche supplémentaire : Harvester Windows
(Recommandé) Modifier les ACL du routeur

Versions de logiciels prises en charge pour la mise à niveau

CA Network Flow Analysis 9.3.0 prend en charge les mises à niveau des versions suivantes vers la configuration actuelle :

- CA Network Flow Analysis 9.2.1
- CA Performance Center 2.4/2.3 ou CA NetQoS Performance Center 6.1.205 SP2/6.1.194
- (Facultatif) CA Anomaly Detector 9.2.1

Source	Mise à niveau vers
NFA 9.2.1 exécuté avec CA PC 2.3.x	NFA 9.3.0 exécuté avec CA PC 2.4/2.3
NFA 9.2.1 exécuté avec NPC 6.1.205 SP2/6.1.194	NFA 9.3.0 exécuté avec NPC 6.1.205 SP2/6.1.194

Lorsque vous mettez à niveau le logiciel, vous continuez à utiliser la même architecture qu'avec la version 9.2.1, comme indiqué dans la liste suivante :

- Autonome vers autonome
- Distribué à 2 niveaux vers distribué à 2 niveaux
- Distribué à 3 niveaux vers distribué à 3 niveaux

CA Network Flow Analysis 9.2.1 est la seule version logicielle que vous pouvez mettre à niveau directement vers la version 9.3.0. Si vous possédez une version antérieure, vous devez procéder à sa mise à niveau vers la version 9.2.1 avant de poursuivre. Pour plus d'informations, consultez le *Manuel de mise à niveau de CA Network Flow Analysis 9.2.1*.

Remarques :

- Mettez à niveau CA Network Flow Analysis avant de mettre à niveau Performance Center.
- N'installez pas et ne mettez pas à niveau un composant CA Network Flow Analysis sur un serveur sur lequel vous avez installé Performance Center. La console NFA ou le déploiement autonome peuvent coexister avec CA Anomaly Detector, mais avec aucun autre logiciel.

- Si vous envisagez de basculer entre CA NetQoS Performance Center (NPC) et CA Performance Center (CA PC), annulez l'enregistrement avant de mettre à niveau CA Network Flow Analysis. Annulez l'enregistrement avant de passer de NPC à CA PC ou inversement.
- Le protocole NTLM (Windows NT LAN Manager) n'est pas pris en charge par l'outil d'authentification unique.

Téléchargement des fichiers de mise à niveau

Copiez les fichiers d'installation ou de mise à niveau sur le serveur d'installation afin d'être sûr de pouvoir y accéder à tout moment.

1. Procurez-vous les fichiers d'installation ou de mise à niveau des composants :
   a. Connectez-vous au site support.ca.com.
   b. Accédez au centre de téléchargement, en accédant au menu Support dans le volet gauche et en cliquant sur Download Center (Centre de téléchargement) par exemple.
   c. Sélectionnez les options de navigation suivantes :
      - Sélectionnez un produit : sélectionnez CA Network Flow Analysis - MULTI-PLATFORM pour afficher les liens de la console NFA, du Harvester (Windows), du Harvester (Linux), de l'appliance DSA et des fichiers ISO d'installation et de mise à niveau de CA Anomaly Detector.
      - Select a Release (Sélectionner une version) : sélectionnez 9.3.
      - Select a Gen level (Sélectionner un niveau de génération) : sélectionnez 0000.
   d. Téléchargez les fichiers ISO dans la liste de composants du produit (Product Components) qui apparaît.

      Remarque : Un fichier ISO est un fichier d'archive qui contient le contenu d'un disque optique. Chacun des fichiers ISO disponibles contient les fichiers d'installation ou de mise à niveau du composant indiqué dans le lien du fichier.
2. Effectuez l'une des tâches suivantes :
   - Gravez les fichiers ISO sur un CD-ROM ou un DVD.
   - Extrayez le contenu des fichiers ISO à l'aide d'une application logicielle d'image ISO. Les applications gratuites de création d'images ISO sont nombreuses.
3. Extrayez les fichiers appropriés sur les serveurs d'installation :
   - Serveurs autonomes :
      - NFHarvesterSetup9.3.0.exe
      - RAConsoleSetup9.3.0.exe

- Serveurs de Harvester Windows dans des déploiements distribués :
  - NFHarvesterSetup9.3.0.exe
- – Serveurs de Harvester Linux dans des déploiements distribués :
  - NFHarvesterSetup9.3.0.bin
- – Serveurs de console NFA dans des déploiements distribués :
  - RAConsoleSetup9.3.0.exe
- – Serveurs de DSA dans des déploiements distribués à trois niveaux :
  - DSASetup9.3.0.exe

Vous pouvez installer ou mettre à niveau le logiciel localement ou à distance.

Chapitre 2: Recommandations système et configuration requise

Cette section décrit les configurations, le matériel et le système d'exploitation requis pour les serveurs de composant CA Network Flow Analysis.

Ce chapitre traite des sujets suivants :

Configuration requise pour les systèmes d'exploitation Windows

Vous pouvez installer et mettre à niveau le logiciel CA Network Flow Analysis 9.3.0 sur des serveurs munis des systèmes d'exploitation suivants :

- Windows Server 2008 R2 Standard Edition (tous les composants)

  Pour obtenir de l'aide pour la mise à niveau de votre système d'exploitation Windows en vue de la mise à niveau du logiciel, contactez le support technique de CA.

- Red Hat Enterprise Linux 5.5 ou 5.6 (Harvester)

Si vous ajoutez de nouveaux serveurs de composant à votre déploiement, assurez-vous qu'ils sont dotés de l'un des systèmes d'exploitation suivants :

- Harvester : Windows Server 2008 R2 Standard Edition ou Red Hat Enterprise Linux 5.5 ou 5.6
- DSA : Windows Server 2008 R2 Standard Edition

Les serveurs doivent disposer des éléments requis suivants :

- Service Pack le plus récent et les principales mises à jour importantes
- Anglais, chinois (simplifié), français (France) ou japonais

  Packs linguistiques appropriés sur tous les serveurs pour les déploiements dans une version localisée

- Résolution d'affichage de 1024x768 (XGA) minimum

- Les mises à niveau vers CA Network Flow Analysis 9.3.0 requièrent de l'espace supplémentaire pour la migration et la sauvegarde de la base de données. Pour déterminer l'espace requis, procédez comme suit :

  1. Localisez le répertoire CA/NFA/MySql51/data.
  2. Déterminez la taille du répertoire.
  3. Pour calculer l'espace libre requis sur le disque, additionnez la taille du répertoire et celle de l'installation du produit 9.3.0 (environ 1,5 Go).

- Configuration serveur décrite dans les sections :

  – Respect des conditions par les serveurs Windows (page 21)

  – Tâches postérieures à la mise à niveau (page 65)

Remarques :

- Avant d'effectuer les tâches indiquées dans ce manuel, connectez-vous à un serveur Windows en tant qu'utilisateur membre du groupe Administrateurs ou à un serveur Linux avec des droits d'utilisateur root.
- CA Network Flow Analysis 9.3.0 prend en charge les installation et mises à niveau sur des serveurs utilisant une adresse IPv4 et pas IPv6.
- Il est recommandé de configurer un contrôleur d'interface réseau unique sur chaque serveur.
- La configuration requise et les recommandations indiquées dans cette section s'appliquent aussi bien aux déploiements physiques que virtuels.

Si l'une des situations spéciales suivantes se présente, faites appel à votre responsable support désigné CA :

- DSA sous Linux : migration de DSA Linux vers des serveurs Windows
- Changement du lecteur d'installation : déplacement du dossier d'installation d'un composant vers un nouveau lecteur

Matériel pour le serveur Windows

Dans un déploiement *distribué*, les composants CA Network Flow Analysis sont installés sur des serveurs distincts.

Un *serveur autonome* est un serveur unique utilisé pour l'installation de tous les composants CA Network Flow Analysis.

Nous avons testé le produit avec la configuration matérielle suivante. La configuration requise peut varier selon les caractéristiques et le volume d'interfaces, d'applications et d'opérateurs présents sur votre réseau.

Remarques :

- Les spécifications recommandées ci-dessous s'appliquent aux déploiements physiques et virtuels. Les spécifications représentent la configuration optimale, par exemple la configuration des appliances CA actuellement fournies. Vous pouvez exécuter CA Network Flow Analysis sur des configurations qui ne répondent pas à ces spécifications, mais les performances s'en verront affectées.
- Pour obtenir de meilleures performances, exécutez le logiciel et le système d'exploitation sur des lecteurs distincts. Il est toutefois possible d'installer et d'exécuter le logiciel et le système d'exploitation sur le même lecteur.

Les recommandations suivantes s'appliquent aux serveurs dédiés qui sont utilisés pour installer un ou plusieurs composants CA Network Flow Analysis :

Serveur autonome ou de la console NFA

- Processeur quadruple coeur de 2,26 GHz
- 3 Go de mémoire RAM
- Trois disques durs SAS de 146 Go et 10 000 tr/min en configuration RAID 5
- Port Ethernet de 1 Go
- Partition pour le lecteur C avec 40 Go d'espace disponible pour le système d'exploitation
- Partition sur un lecteur qui contient 41 Go d'espace disponible pour les fichiers d'installation/mise à niveau et au moins 200 Go pour les données

Serveur du Harvester

- Deux processeurs quadruple coeur de 2,26 GHz
- 12 Go de RAM
- Six disques durs SAS de 300 Go et 10 000 tr/min en configuration RAID 5
- Port Ethernet de 1 Go

- Partition pour le lecteur C avec 40 Go d'espace disponible pour le système d'exploitation
- Partition sur un lecteur qui contient 41 Go d'espace disponible pour les fichiers d'installation/mise à niveau et 1 To pour les données

Serveur d'appliance de stockage de données (DSA) (architecture à trois niveaux uniquement)

- Processeur quadruple coeur de 2,26 GHz
- 12 Go de RAM
- Six disques durs SAS de 300 Go et 10 000 tr/min en configuration RAID 5
- Port Ethernet de 1 Go
- Partition pour le lecteur C avec 40 Go d'espace disponible pour le système d'exploitation
- Partition sur un lecteur qui contient 41 Go d'espace disponible pour les fichiers d'installation/mise à niveau et 1 To pour les données

Matériel et système d'exploitation pour le serveur Linux

Pour un déploiement distribué, CA Network Flow Analysis prend en charge l'exécution du Harvester sur des serveurs Linux dédiés disposant de la configuration requise suivante :

- Red Hat Enterprise Linux 5.5 ou 5.6 sur un processeur 64 bits
- Anglais, chinois (simplifié), français (France) ou japonais

  Packs linguistiques appropriés sur tous les serveurs pour les déploiements dans une version localisée

Nous conseillons d'utiliser des serveurs de Harvester Linux remplissant les spécifications suivantes :

- Deux processeurs quadruple coeur de 2,26 GHz
- 12 Go de RAM
- Six disques durs SAS de 300 Go et 10 000 tr/min en configuration RAID 5
- Port Ethernet de 1 Go
- Partition racine comprenant 40 Go d'espace disponible
- Partition pour CA Network Flow Analysis comprenant l'espace suivant :
  - 41 Go pour les fichiers d'installation ou de mise à niveau
  - 1 To pour les données

Si vous ne disposez pas d'assez d'espace disponible au niveau du répertoire /tmp et que vous ne pouvez pas configurer ce répertoire, déplacez-le. Exportez la variable d'environnement IATEMPDIR, pour définir un nouvel emplacement pour le répertoire temporaire Install Anywhere et sélectionnez un répertoire avec l'espace suffisant.

Remarques :

- CA Network Flow Analysis 9.3.0 prend en charge l'installation sur des serveurs avec des adresses IPv4. L'installation des serveurs avec des adresses IPv6 n'est pas encore prise en charge.
- Les spécifications décrites dans cette section s'appliquent aussi bien aux déploiements physiques que virtuels.

Chapitre 3: Préparation des serveurs Windows

Ce chapitre traite des sujets suivants :

Respect des conditions par les serveurs Windows

Avant de commencer la mise à niveau, vérifiez les conditions suivantes. Le non-respect de ces conditions peut entraîner une perte des données, une augmentation des temps d'arrêt, des conflits de logiciels ou un échec de la mise à niveau.

Vérifiez les conditions suivantes :

- Les serveurs d'installation incluent des installations complètement opérationnelles du logiciel CA Network Flow Analysis pris en charge pour la mise à niveau (page 11).
- Votre déploiement inclut une version prise en charge de Performance Center (page 66).
- Les serveurs Windows présentent la configuration requise indiquée dans le tableau ci-dessous.

Stand-Alone Server (Serveur JDBC)	Serveur de console NFA distribué	Serveur de Harvester distribué	Serveur de DSA à 3 niveaux distribué
■ La configuration système requise par les systèmes d'exploitation Windows est remplie. (page 15)			
■ (Recommandé) Les recommandations au niveau du matériel Windows (page 17) sont remplies.			
■ (Recommandé) L'option Connexion Bureau à distance est activée pour permettre l'accès à distance.			
■ Les exécutables de mise à niveau sont téléchargés vers les serveurs (page 12).			
■ Une adresse IP statique est affectée à chaque serveur. Définition de l'adresse IP du serveur de Harvester sur la destination d'exportation des flux affectée à chaque routeur			
■ Une version prise en charge de .NET Framework est installée (page 24)*			
■ (Recommandé) Le navigateur pris en charge (page 23) est installé.**			
■ Les pare-feu sont configurés. (page 24)			
■ IIS, COM+ et ASP (page 28) sont installés.**			
■ Le paramètre SNMP (page 30) est configuré.**			
■ Les adresses IPv6 sont désactivées. (page 32)			
■ La fonctionnalité de prévention de l'exécution des données est configurée. (page 33)			
■ Les logiciels tiers suivants sont désactivés jusqu'à la fin de la mise à niveau : logiciels antivirus, de surveillance de serveur et de maintenance. Si vous activez des analyses antivirus ultérieurement, excluez le répertoire d'installation CA Network Flow Analysis et ses sous-répertoires.			
■ Les bases de données sont vérifiées. (page 41)			
■ Les services sont arrêtés (page 43), les bases de données sont sauvegardées et les services sont redémarrés.			

*Cette condition est requise pour que le programme de mise à niveau puisse s'ouvrir ou s'exécuter.
**Si cette condition n'est pas remplie sur le serveur, un message d'avertissement s'affiche.

Remarques d'ordre général :

- Empêchez d'autres programmes de s'exécuter lors de l'installation ou de la mise à niveau.
- Lorsque vous appliquez des mises à jour Windows, redémarrez tous les serveurs pour garantir l'application des mises à jour.
- Vérifiez que personne d'autre n'est connecté au serveur pendant l'installation ou la mise à niveau.

Remarques relatives à la localisation :

- Pour permettre la prise en charge des caractères non-latins, comme le chinois simplifié et le japonais, les clients de ligne de commande que vous utilisez pour l'installation doivent être configurés pour permettre le codage UTF-8. Ces caractères peuvent ne pas s'afficher correctement lorsque le codage UTF-8 n'est pas activé.
- Les packs linguistiques appropriés sont requis lors des déploiements des versions localisées.
- Les paramètres régionaux doivent utiliser un point (.) pour indiquer une valeur décimale. Si votre déploiement est localisé en français, remplacez le symbole décimal par un point dans la boîte de dialogue Région et langue : Personnaliser le format.

Navigateurs Web pris en charge

Pour les systèmes clients utilisés pour se connecter à la console NFA, nous recommandons la version 8 de Microsoft Internet Explorer. D'autres navigateurs ou versions de navigateur peuvent fonctionner avec la console NFA, mais ils n'ont pas été testés.

Pour les systèmes d'installation : si vous installez un navigateur, installez la version 8 de Microsoft Internet Explorer.

Requis/facultatif	Navigateurs pris en charge	Serveurs à configurer
Navigateur requis	Internet Explorer 8 recommandé	Systèmes utilisés pour la connexion à la console NFA
Navigateur facultatif	Internet Explorer 8 requis si un navigateur est installé	Serveurs d'installation

Pour configurer CA Network Flow Analysis et utiliser ses données dans la console CA Performance Center, utilisez Internet Explorer et désactivez l'affichage de compatibilité. L'utilisation d'Internet Explorer dans la console NFA ne requiert pas la désactivation de l'affichage de compatibilité.

Si les outils de développement Internet Explorer ont été installés, vous pouvez utiliser la touche F12 pour accéder aux options Affichage de compatibilité correspondant à la session de navigateur actuelle :

1. Appuyez sur la touche F12.

   Un nouveau volet s'ouvre dans la partie inférieure de la fenêtre.

2. Cliquez sur l'élément Mode navigateur dans le menu principal.
3. Sélectionnez l'option Internet Explorer qui ne contient pas l'expression "Affichage de compatibilité".

Remarques :

- Pour plus d'informations sur les versions de navigateur, consultez le *Fichier Readme*.
- Pour plus d'informations sur la configuration du navigateur sur le serveur de la console CA NetQoS Performance Center, reportez-vous à la rubrique Configuration d'Internet Explorer dans le Manuel d'installation de CA NetQoS Performance Center.

Installation de .NET Framework

Installez .NET Framework 3.5.1 sur tous les serveurs Windows en vous connectant en tant qu'utilisateur membre du groupe Administrateurs.

Si le logiciel .NET Framework est manquant, le programme d'installation ou de mise à niveau se ferme suite à la vérification des éléments requis.

Requis/facultatif	Serveurs à configurer
Obligatoire	Tous les serveurs

Configuration du pare-feu

Pour que CA Network Flow Analysis fonctionne correctement dans un environnement protégé par un pare-feu, certains ports doivent être ouverts. Les rubriques suivantes répertorient les ports qui doivent être ouverts pour permettre aux composants CA Network Flow Analysis de communiquer. Pour cela, connectez-vous en tant qu'utilisateur membre du groupe Administrateurs.

- Système autonome (page 25)
- Déploiement distribué à deux niveaux (page 25)
- Déploiement distribué à trois niveaux (page 26)

Ports à ouvrir pour un système autonome

Ouvrez les ports suivants sur un système autonome pour permettre le fonctionnement sans heurt des communications CA Network Flow Analysis.

Source	Destination	Port [Fonction]
Console NFA	Sortant	■ TCP 25 [rapports par courriel SMTP] ■ UDP 53 [DNS]
Harvester	Routeurs (interface SNMP, lecture seule)	■ UDP 161 [interrogation SNMP]
Harvester	Destination des interruptions	■ UDP 162 [interruptions]
Routeur	Harvester	■ UDP 9995 [flux]
Administrateurs et opérateurs	Console NFA	■ TCP/HTTP 80 [accès IUG et services Web SNMP] ■ TCP/HTTP 8381 [authentification unique]
Console CA PC/NPC	Console NFA	■ TCP/HTTP 80 [synchronisation des unités et interfaces avec CA PC/NPC] ■ TCP 8681 [importation de données pour les vues NFA dans CA PC/NPC]
Administrateurs	Chaque serveur	■ TCP 3389 [ordinateur de bureau distant, si un ordinateur Distant est utilisé] ■ TCP 5800, 5801, 5900, 5901 [VNC, si VNC est activé]

Ports à ouvrir pour un déploiement distribué à deux niveaux

Déploiement distribué à deux niveaux

Console NFA et Harvesters sur des serveurs distincts, sans DSA

Ouvrez les ports suivants dans un déploiement distribué à deux niveaux pour permettre la communication entre la console NFA, les Harvesters et d'autres éléments.

Source	Destination	Port [Fonction]
Console NFA	Sortant	■ TCP 25 [rapports par courriel SMTP] ■ UDP 53 [DNS]

Source	Destination	Port [Fonction]
Console NFA	Harvester	■ TCP 3307 [CA MySQL] ■ TCP 3308 [MySQL] ■ TCP 8066 [appels services Web SOAP] ■ TCP 8080 [port de serveur Web de fichiers pour la collecte des fichiers de Harvester] ■ UDP 161 [service de surveillance]
Harvester	Routeurs (interface SNMP, lecture seule)	■ UDP 161 [interrogation SNMP]
Harvester	Destination des interruptions	■ UDP 162 [interruptions]
Routeur	Harvester	■ UDP 9995 [flux]
Administrateurs et opérateurs	Console NFA	■ TCP/HTTP 80 [accès IUG et services Web SNMP] ■ TCP/HTTP 8381 [authentification unique]
Console CA PC/NPC	Console NFA	■ TCP/HTTP 80 [synchronisation des unités et interfaces avec CA PC/NPC] ■ TCP 8681 [importation de données pour les vues NFA dans CA PC/NPC]
Administrateurs	Chaque serveur	■ TCP 3389 [ordinateur de bureau distant, si un ordinateur Distant est utilisé] ■ TCP 5800, 5801, 5900, 5901 [VNC, si VNC est activé]

Ports à ouvrir pour un déploiement distribué à trois niveaux

Déploiement distribué à trois niveaux

Console NFA, Harvester et DSA sur des serveurs distincts

Ouvrez les ports suivants dans un déploiement distribué à trois niveaux pour permettre la communication entre la console NFA, les Harvesters, les DSA et autres éléments.

Source	Destination	Port [Fonction]
Console NFA	Sortant	■ TCP 25 [rapports par courriel SMTP] ■ UDP 53 [DNS]

Source	Destination	Port [Fonction]
Console NFA	Harvester	■ TCP 3307 [CA MySQL] ■ TCP 3308 [MySQL] ■ TCP 8066 [appels services Web SOAP] ■ TCP 8080 [port de serveur Web de fichiers pour la collecte des fichiers de Harvester] ■ UDP 161 [service de surveillance]
Console NFA	DSA	■ TCP 3307 [CA MySQL] ■ TCP 3308 [MySQL] ■ UDP 161 [service de surveillance]
Harvester	Routeurs (interface SNMP, lecture seule)	■ UDP 161 [interrogation SNMP]
Harvester	Destination des interruptions	■ UDP 162 [interruptions]
DSA	Console NFA	■ TCP 3308 [MySQL] ■ TCP 8080 [service Web de fichiers qui récupère des fichiers de la console NFA sans utiliser de partage de fichiers]
Routeur	Harvester	■ UDP 9995 [flux]
Administrateurs et opérateurs	Console NFA	■ TCP/HTTP 80 [accès IUG et services Web SNMP] ■ TCP/HTTP 8381 [authentification unique]
Console CA PC/NPC	Console NFA	■ TCP/HTTP 80 [synchronisation des unités et interfaces avec CA PC/NPC] ■ TCP 8681 [importation de données pour les vues NFA dans CA PC/NPC]
Administrateurs	Chaque serveur	■ TCP 3389 [ordinateur de bureau distant, si un ordinateur Distant est utilisé] ■ TCP 5800, 5801, 5900, 5901 [VNC, si VNC est activé]

Installation de IIS, de ASP et COM+

Procédez aux étapes indiquées dans cette rubrique pour installer les composants requis suivants sur un serveur autonome ou sur un serveur de console NFA :

- IIS
- ASP
- IIS 6 Management Compatibility
- COM+ Network Access

Requis/facultatif	Serveurs à configurer
Obligatoire	Autonome, de console

Procédez comme suit :

1. Connectez-vous en tant qu'utilisateur possédant des droits d'administration au niveau de CA Network Flow Analysis.
2. Sélectionnez Démarrer, Outils d'administration, Gestionnaire de serveur.

   La fenêtre Gestionnaire de serveur s'ouvre.
3. Développez la liste Rôles dans l'arborescence Console à gauche.
4. Ajoutez le service de rôle IIS :
   a. Cliquez sur le lien Serveur d'applications dans la liste Rôles de l'arborescence Console à gauche.

      La vue Serveur d'applications s'ouvre dans le volet droit.

   b. Dans la section Services de rôle, cliquez sur Ajouter des services de rôle.

      L'Assistant Ajouter des services de rôle s'ouvre à la page Sélectionner les services de rôle.

   c. Cochez la case Prise en charge du serveur Web (IIS).

   d. Dans le message de confirmation qui s'affiche, cliquez sur Ajouter les services de rôle requis.

      L'option Prise en charge du serveur Web (IIS) est mise en surbrillance dans la page Sélectionner les services de rôle.
5. Ajoutez le service de rôle COM+ :
   a. Cochez la case Accès réseau COM+.

   b. Dans le message de confirmation qui s'affiche, cliquez sur Ajouter les services de rôle requis, puis sur Suivant.

      La page Serveur Web (IIS) de l'Assistant Ajouter des services de rôle s'ouvre.

6. Activez IIS 6 Management Compatibility :
   a. Cliquez à nouveau sur Suivant.

      Une liste de services de rôle s'ouvre.
   b. Dans la section Outils de gestion, activez l'option Compatibilité avec la gestion IIS 6.
   c. Cliquez sur Suivant.

      La page Confirmer les sélections pour l'installation récapitule vos actions et affiche les messages associés.
7. Installez les options et les rôles de service IIS et COM+ que vous avez sélectionnés :
   a. Cliquez sur Installer.

      La page Résultats s'ouvre lorsque l'installation ou la mise à niveau est terminée.
   b. (Facultatif) Cliquez sur Imprimer, envoyer ou enregistrer le rapport d'installation/de mise à niveau, vérifiez les informations, puis fermez la page.
   c. Cliquez sur Fermer.

      La page Résultats se ferme.
8. Ajoutez et installez le service de rôle ASP :
   a. Dans l'arborescence Console, allez sous Rôles et cliquez sur le lien Serveur Web (IIS).

      La vue Serveur Web (IIS) s'ouvre dans le volet droit.
   b. Dans la section Services de rôle, cliquez sur Ajouter des services de rôle.

      L'Assistant Ajouter des services de rôle s'ouvre à la page Sélectionner les services de rôle.
   c. Dans la liste, cochez la case ASP sous Développement d'applications et cliquez sur Suivant.

      La page Confirmer les sélections pour l'installation récapitule vos actions et les messages associés.
   d. Cliquez sur Installer.

      La page Résultats s'ouvre lorsque l'installation ou la mise à niveau est terminée.
   e. (Facultatif) Cliquez sur Imprimer, envoyer ou enregistrer le rapport d'installation/de mise à niveau, vérifiez les informations, puis fermez la page.
   f. Cliquez sur Fermer.

      La page Résultats de l'installation se ferme.
9. Quittez la fenêtre Gestionnaire de serveur.

Configuration de SNMP sur les serveurs Windows

Le service Simple Network Management Protocol (SNMP) est requis par les services de surveillance. Procédez comme indiqué dans cette rubrique pour configurer le service SNMP sur les serveurs Windows présents dans votre déploiement.

Requis/facultatif	Serveurs à configurer
Obligatoire	Tous les serveurs

Procédez comme suit :

1. Connectez-vous en tant qu'utilisateur possédant des droits d'administration au niveau de CA Network Flow Analysis.
2. Ouvrez la fenêtre Gestionnaire de serveur, sélectionnez Démarrer, Outils d'administration, puis Gestionnaire de serveur.
3. Installez les services SNMP :
    a. Cliquez sur Fonctionnalités dans le volet de gauche.

       La fenêtre Gestionnaire de serveur affiche une liste des fonctionnalités installées.

    b. Cliquez sur Ajouter des fonctionnalités dans le volet droit.

       L'assistant Ajouter des fonctionnalités s'ouvre et affiche la liste des fonctionnalités sélectionnées et disponibles.

    c. Activez l'option Services SNMP.

       Un message de confirmation apparaît.

    d. Cliquez sur Ajouter les fonctionnalités requises.

       La page de services Confirmer l'installation identifie les fonctionnalités à installer et affiche des messages.

    e. Cliquez sur Installer.

       La page Résultats de l'installation s'ouvre lorsque l'installation ou la mise à niveau est terminée.

4. Quittez la fenêtre Gestionnaire de serveur :
    a. Cliquez sur Fermer.

       Un message vous demande si vous voulez redémarrer le serveur.

    b. Cliquez sur Oui.

       Une fois le serveur redémarré, la vue Fonctionnalités de la fenêtre Gestionnaire de serveur contient les dernières fonctionnalités installées.

5. Affichez la liste de noms de communauté pour le service SNMP :

   a. Sélectionnez Démarrer, Outils d'administration, Services.

      La fenêtre Services s'affiche.

   b. Cliquez avec le bouton droit sur le service SNMP et sélectionnez Propriétés

      La boîte de dialogue Propriétés du service s'ouvre.

   c. Sélectionnez l'onglet Sécurité.

6. Vérifiez que le nom de communauté approprié figure dans la liste Noms de communautés acceptés. Le nom de communauté par défaut est public.

7. Si le nom de communauté approprié ne se trouve pas dans la liste, ajoutez-le en procédant comme suit :

   a. Cliquez sur Ajouter.

      La boîte de dialogue Configuration du service SNMP s'ouvre.

   b. Spécifiez les options suivantes :

      - Droits de communauté : sélectionnez Lecture seule.
      - Nom de communauté : saisissez **public** ou un nom de communauté personnalisé. Utilisez le même nom de communauté tout au long du déploiement de CA Network Flow Analysis :

        Fichier snmpd.conf sur chaque serveur Linux

        Service SNMP sur chaque serveur Windows

        Page de paramètres de l'outil de surveillance de la console NFA

   c. Cliquez sur Ajouter.

      La boîte de dialogue Configuration du service SNMP se ferme. La boîte de dialogue Propriétés du service SNMP affiche le nouveau nom dans la liste Noms de communautés acceptés.

8. Enregistrez vos modifications et quittez le programme :

   a. Dans la boîte de dialogue des propriétés de service SNMP, cliquez sur OK.

      Vos modifications sont enregistrées et la boîte de dialogue se ferme.

   b. Dans la fenêtre Services, sélectionnez Fichier, puis Quitter.

      La fenêtre Services se ferme.

Désactivation des connexions IPv6 sur les serveurs Windows

Cette version ne prend pas en charge les connexions à des adresses de type IPv6. Cette rubrique décrit la procédure à suivre pour configurer les systèmes Windows Server 2008 afin qu'ils ne se connectent pas aux adresses IPv6. En effet, si la connexion aux adresses IPv6 est activée, la collecte de données échoue.

Requis/facultatif	Serveurs à configurer
Recommandé	Tous les serveurs

Les instructions suivantes ne sont effectives que si la configuration recommandée est respectée, c'est-à-dire qu'une carte d'interface réseau unique est configuré pour chaque serveur.

Procédez comme suit :

1. Connectez-vous en tant qu'utilisateur possédant des droits d'administration au niveau de CA Network Flow Analysis.
2. Ouvrez la fenêtre Connexions réseau :
   a. Dans le menu Démarrer, sélectionnez Panneau de configuration.
   b. Dans le Panneau de configuration, cliquez sur Réseau et Internet.
   c. Dans la fenêtre Réseau et Internet qui s'ouvre, cliquez sur Centre Réseau et partage.
   d. Dans la partie gauche de la fenêtre Centre Réseau et partage qui s'ouvre, cliquez sur Modifier les paramètres de la carte.

      La fenêtre Connexions réseau s'ouvre et indique les connexions actuellement configurées.
3. Cliquez avec le bouton droit de la souris sur la connexion.
4. Sélectionnez Propriétés dans le menu.

   La boîte de dialogue Propriétés s'affiche.
5. Le cas échéant, désactivez l'option Protocole Internet version 6 (TCP/IPv6).
6. Cliquez sur OK.

   La boîte de dialogue se ferme et vos modifications sont enregistrées.
7. Dans la fenêtre Connexions réseau, sélectionnez Organiser, puis Fermer.

   La fenêtre se ferme.

Configuration de la prévention de l'exécution des données (PED)

La stratégie Prévention de l'exécution des données (PED) vous aide à empêcher l'exécution de code à partir des pages de données. Cette rubrique décrit la procédure à suivre pour configurer le niveau de stratégie PED approprié.

Requis/facultatif	Serveurs à configurer
Obligatoire	Tous les serveurs

Procédez comme suit :

1. Connectez-vous en tant qu'utilisateur possédant des droits d'administration au niveau de CA Network Flow Analysis.
2. Ouvrez le Panneau de configuration et cliquez sur le lien Système.
3. Dans la boîte de dialogue Propriétés système qui s'ouvre, cliquez sur l'onglet Avancé.
4. Cliquez sur Paramètres.
5. Dans la boîte de dialogue Options de performance qui s'ouvre, cliquez sur l'onglet Prévention de l'exécution des données.
6. Sélectionnez Activer la prévention d'exécution des données pour les programmes et les services Windows uniquement.
7. Enregistrez vos paramètres et quittez le programme :
   a. Cliquez sur OK dans la boîte de dialogue Options de performances.
   b. Cliquez sur OK dans la boîte de dialogue Propriétés système.

      Un message s'ouvre et vous informe que vous devez redémarrer votre système pour que les nouveaux paramètres prennent effet.
8. (Facultatif) Redémarrez votre système avant d'installer ou de mettre à niveau le logiciel.

   Si vous continuez l'installation ou la mise à niveau du logiciel sans redémarrer le système, le test des éléments requis affiche un avertissement concernant la configuration de la PED.

Préparation en vue de la modification de la version de Performance Center

La console NFA ou le serveur autonome doivent être enregistrés en tant que source de données pour une version prise en charge de CA Performance Center (CA PC) ou CA NetQoS Performance Center (NPC). Si vous envisagez de basculer entre NPC et CA PC, préparez l'opération en procédant comme décrit dans la rubrique suivante :

1. Préparez le système en vue de l'annulation de l'enregistrement de votre version actuelle de Performance Center en procédant comme décrit ci-dessous.
2. Annulation de l'enregistrement de Performance Center
3. Procédez à la mise à niveau de CA Network Flow Analysis.

Important : Nous déconseillons d'annuler l'enregistrement. En effet, l'annulation de l'enregistrement et le réenregistrement entraînent la perte d'une grande partie des personnalisations. Lisez attentivement cette rubrique pour préparer ces événements.

Instructions générales

- Si vous devez mettre à niveau CA Performance Center vers la version 2.4, mettez d'abord à niveau CA Network Flow Analysis.
- Si vous envisagez de basculer entre différentes versions de Performance Center, annulez l'enregistrement avant de mettre à niveau CA Network Flow Analysis. Par exemple, annulez l'enregistrement avant de passer de CA NetQoS Performance Center à CA Performance Center ou de CA Performance Center à CA NetQoS Performance Center.

Résultats de l'annulation de l'enregistrement dans CA NetQoS Performance Center

Les règles suivantes s'appliquent en cas d'annulation de l'enregistrement de CA Network Flow Analysis dans CA NetQoS Performance Center suivie de l'enregistrement du produit dans CA Performance Center :

- Domaines :
  - Le domaine par défaut est conservé. Les groupes, les utilisateurs, les unités (routeurs), les interfaces, les noms de protocole et les étiquettes de types de services affectés au domaine par défaut conservent leurs affectations.
  - Les domaines personnalisés sont supprimés.
  - Les groupes, les utilisateurs, les unités (routeurs) et les interfaces appartenant à des domaines personnalisés sont réaffectés au domaine par défaut.
  - Les noms de protocoles, les étiquettes de types de service, les noms de systèmes autonomes et les adresses IP de domaines personnalisés deviennent inaccessibles.

- Comptes d'utilisateur :
  - Les comptes d'utilisateurs sont conservés si les utilisateurs disposent de paramètres de droit d'accès au produit valides (utilisateur, utilisateur avancé ou administrateur) pour CA Network Flow Analysis. Les comptes d'utilisateurs sans droits d'accès au produit pour CA Network Flow Analysis sont supprimés.
  - Les comptes d'utilisateurs associés à des domaines personnalisés seront associés au domaine par défaut.
  - Si le compte d'utilisateur nqadmin existe et comprend un droit d'accès au produit inférieur au droit Administrateur, ce compte d'utilisateur acquiert le droit d'accès au produit Administrateur.

  Vous ne pouvez pas ajouter de nouveaux utilisateurs ou modifier les paramètres des comptes d'utilisateurs après l'annulation de l'enregistrement.
- Rôles :
  - Les rôles personnalisés et par défaut sont conservés et restent associés aux comptes d'utilisateurs.
- Groupes : ils sont conservés si les conditions suivantes sont remplies.
  - Le groupe est un groupe par défaut dans CA NetQoS Performance Center ou un groupe ajouté à CA NetQoS Performance Center. Les groupes dynamiques, tels que les groupes interproduit, sont supprimés.
  - Le groupe contient des données (il n'est pas vide).

  Les groupes par défaut et personnalisés requièrent le nettoyage de la page Gérer les groupes dans CA Performance Center après avoir annulé l'enregistrement et avoir réenregistré le nouveau logiciel. Les changements suivants peuvent apparaître :
  - Certains noms de groupes sont légèrement modifiés. Par exemple, le groupe Toutes les interfaces est renommé Interfaces.
  - Les structures peuvent être réduites de sorte qu'un groupe intégré à un autre groupe en soit retiré.
  - Les groupes peuvent être déplacés :

    Un groupe personnalisé qui apparaissait initialement sur la page Gérer les groupes sous Tous les groupes/Groupes système/Sources de données/ReporterAnalyzer se retrouve sous Network Flow Analysis dans la nouvelle arborescence de groupes. Le nouvel emplacement est Tous les groupes/Inventaire/Sources de données/Network Flow Analysis.

    Si le groupe personnalisé ne se trouvait initialement pas sous ReporterAnalyzer, il est déplacé vers Network Flow Analysis.
  - Des groupes dupliqués peuvent être créés.
  - Les groupes personnalisés vides sont supprimés.

- Profils SNMP : les profils SNMP de CA NetQoS Performance Center 6.1.205 SP2/6.1.194 sont conservés et leur statut n'est pas modifié.
- Personnalisations de l'authentification unique : les personnalisations de l'authentification unique LDAP et autres sont conservées.

  Si vous basculez vers une nouvelle version de l'application d'authentification unique, mettez à jour les paramètres de configuration de l'authentification unique en procédant comme décrit dans le *Manuel de l'utilisateur de l'authentification unique*.

Procédez comme suit :

1. Connectez-vous à la console CA NetQoS Performance Center en tant qu'utilisateur membre du groupe Administrateurs.
2. Révisez vos enregistrements des personnalisations dans CA NetQoS Performance Center, notamment ceux ci-dessous :
   - Comptes d'utilisateurs et leurs rôles, autorisations du produit, groupes et accès au domaine
   - Rôles personnalisés et rôles standard personnalisés, y compris toute affectation pour les menus de niveau supérieur, les tableaux de bord et les menus de tableau de bord
   - Structure de groupe et conventions d'attribution de nom
   - Domaines personnalisés et leur contenu, comme les groupes, les unités, les interfaces, les profils SNMP, dossiers de rapports, les noms de systèmes autonomes, les noms de protocoles, les étiquettes de types de services et les adresses IP

   Ces éléments peuvent requérir une vérification, une restructuration ou une restauration.
3. (Facultatif) Préparation à l'annulation de l'enregistrement :

   Vous pouvez attribuer un nom unique à chaque groupe afin de faciliter la restauration de la hiérarchie de groupes, en décrivant sa relation par rapport à d'autres groupes par exemple.

   Pour garantir qu'aucun groupe n'est supprimé, aplanissez la hiérarchie de groupes avant de procéder à l'annulation de l'enregistrement.
4. Ouvrez la page Data Source List (Liste des sources de données) : cliquez sur Admin (Administration), sur NetQoS Settings (Paramètres de NetQoS), puis sur Data Sources (Sources de données).
5. Sélectionnez la source de données de CA Network Flow Analysis ou ReporterAnalyzer.
6. Cliquez sur Supprimer.

Chapitre 4: Préparation des serveurs Linux

Ce chapitre traite des sujets suivants :

Respect des conditions par les serveurs Linux

Avant de commencer la mise à niveau, vérifiez les conditions suivantes. Le non-respect de ces conditions peut entraîner une perte des données, une augmentation des temps d'arrêt, des conflits de logiciels ou un échec de la mise à niveau.

- Configuration système requise : vérifiez que les serveurs de mise à niveau remplissent la configuration système requise et les recommandations pour Linux (page 18).
- Configuration logicielle requise : vérifiez que les serveurs de mise à niveau sont dotés du logiciel CA Network Flow Analysis entièrement opérationnel et pris en charge pour la mise à niveau (page 11).
- Vérifiez que chaque serveur Linux de Harvester est prêt pour la mise à niveau. Pour cela :
  - Affectez une adresse IP statique à chaque serveur. Définition de l'adresse IP du serveur de Harvester sur la destination d'exportation des flux affectée à chaque routeur
  - Configuration de la fonction SNMP (page 38)

    Si SNMP ne s'exécute pas, le programme de mise à niveau affiche un avertissement. Vous pouvez cependant omettre l'avertissement et configurer SNMP après la mise à niveau.
  - Désactivation du pare-feu iptables (page 39)
  - Désactivation de la mise en réseau IPv6 (page 39)
  - Arrêt des services (page 45)
  - Sauvegarde des bases de données (page 46)

- Pour permettre la prise en charge des caractères non-latins, comme le chinois simplifié et le japonais, les clients de ligne de commande que vous utilisez pour l'installation doivent être configurés pour permettre le codage UTF-8. Ces caractères peuvent ne pas s'afficher correctement lorsque le codage UTF-8 n'est pas activé.
- Les packs linguistiques appropriés sont requis lors des déploiements des versions localisées.
- Les paramètres régionaux doivent utiliser un point (.) pour indiquer une valeur décimale. Si votre déploiement est localisé en français, remplacez le symbole décimal par un point dans la boîte de dialogue Région et langue : Personnaliser le format.
- Si la résolution DNS n'est pas configurée, l'interrogation échouera. Pour plus d'informations, reportez-vous au fichier Readme.

Configuration de SNMP sur les serveurs Linux

Pour configurer un serveur Linux pour un Harvester, effectuez les tâches suivantes :

- Si la suite Net-SNMP n'est pas déjà présente sur le serveur d'installation ou de mise à niveau, installez-la en procédant comme décrit dans cette rubrique.
- Une fois l'installation ou la mise à niveau terminée, finalisez la configuration du protocole SNMP : (page 67)
  - Configurez le fichier de configuration Net-SNMP.
  - Configurez SNMP pour qu'il se lance automatiquement lors du démarrage.
  - Lancez le service snmpd.

Vérifiez que la suite Net-SNMP est présente sur le serveur. Dans le cas contraire, installez-la. Net-SNMP est requis pour la prise en charge de la fonctionnalité de surveillance.

Procédez comme suit :

1. Ouvrez le gestionnaire de packages Linux et recherchez les listes qui contiennent net-snmp.

   Si aucune liste ne contient "net-snmp", cela signifie que la suite Net-SNMP n'a pas été installée :

2. Récupérez Net-SNMP et installez-le s'il ne l'est pas déjà. Par exemple, vous pouvez récupérer Net-SNMP à partir du gestionnaire de packages Linux.

Désactivation du pare-feu iptables

Il est recommandé de désactiver le pare-feu iptables et d'arrêter le service iptables sur chaque serveur Linux sur lequel un Harvester est installé. Si vous désactivez les iptables, assurez-vous que tous les ports requis sont ouverts et que les performances ne sont pas affectées.

Remarque : Si votre entreprise requiert l'utilisation d'iptables, vérifiez que tous les ports de pare-feu appropriés sont ouverts dans la liste Configuration du pare-feu (page 24). En outre, vérifiez que vous disposez d'un accès complet depuis l'hôte local à l'hôte local. Cette opération est requise, car CA Network Flow Analysis utilise un accès RMI (appel de méthodes distantes).

Effectuez les opérations suivantes pour désactiver tous les niveaux d'iptables et permettre aux composants CA Network Flow Analysis de communiquer.

Procédez comme suit:

1. Connectez-vous en tant que root ou avec un compte d'utilisateur sudo.
2. Exécutez les commandes suivantes dans une fenêtre d'invite de commande :

```
service iptables stop

chkconfig iptables off

chkconfig –-list |grep iptables
```

3. Examinez la sortie de la dernière commande et vérifiez que tous les niveaux iptables sont désactivés, comme dans l'exemple suivant :

```
iptables 0:off 1:off 2:off 3:off 4:off 5:off 6:off
```

Désactivation de la mise en réseau IPv6 sur les serveurs Linux

Désactivez la mise en réseau IPv6 sur chaque serveur Linux sur lequel un Harvester est installé.

Remarque : Effectuez cette tâche avant d'ajouter le Harvester dans la console NFA. Si le protocole IPv6-format est activé lorsque vous ajoutez un Harvester dans la console NFA, il se lie automatiquement à une adresse IPv6 et les données ne sont pas reçues par CA Network Flow Analysis.

Pour désactiver la mise en réseau IPv6, modifiez les fichiers suivants :

- Le fichier de configuration de pilote de noyau modprobe.conf, qui se trouve par défaut dans le répertoire /etc.
- Le fichier de configuration de pilote RHEL network, qui se trouve par défaut dans le répertoire /etc/sysconfig.

Procédez comme suit :

1. Vérifiez que vous êtes connecté avec les droits root.
2. Modifiez le fichier modprobe.conf :
    a. Ouvrez le fichier /etc/modprobe.conf dans un éditeur de texte.
    b. Ajoutez la ligne suivante :
    ```
    install ipv6 /bin/true
    ```
    c. Enregistrez et fermez le fichier.

    Le fichier modprobe.conf est configuré de façon à ce que lorsque le système essaye de charger le module de noyau IPv6, la commande true est exécutée à sa place. La commande true n'effectue aucune action.
3. Modifiez le fichier réseau :
    a. Ouvrez le fichier /etc/sysconfig/network dans un éditeur de texte.
    b. Mettez à jour les lignes suivantes ou ajoutez-les pour qu'elles correspondent aux chaînes de texte affichées :
    ```
    NETWORKING_IPV6=no
    IPV6INIT=no
    ```
    c. Enregistrez et fermez le fichier.
4. Redémarrez le serveur :
    ```
    reboot
    ```
5. Vérifiez que le protocole IPv6 est désactivé.
    a. Dans un terminal, entrez la commande suivante :
    ```
    lsmod | grep ipv6
    ```
    Si la commande ne renvoie aucune sortie, le module du noyau IPv6 ne s'exécute pas, car il a été supprimé.
    b. Entrez la commande suivante :
    ```
    /sbin/ifconfig
    ```
    Vérifiez que la sortie contient uniquement des adresses IPv4 et aucune adresse IPv6.

Chapitre 5: Vérification et sauvegarde des bases de données

Ce chapitre traite des sujets suivants :

Vérification des bases de données MySQL

Nous vous recommandons de vérifier les tables de base de données avant de procéder à une mise à niveau. En effet, cette opération corrige certains problèmes et permet d'éviter certains problèmes et de ne pas avoir à demander de l'assistance au support CA en matière de récupération. Cette rubrique décrit la procédure d'exécution de la commande mysqlcheck avant la mise à niveau pour vérifier que la configuration des tables de base de données est correcte.

Vous pouvez exécuter la commande mysqlcheck pour vérifier les bases de données suivantes :

- reporter : présente sur chaque serveur autonome ou de la console NFA (qui contient généralement des tables de grande taille)
- harvester : présente sur chaque serveur autonome ou de Harvester
- poller : présente sur chaque serveur autonome ou de Harvester
- data_retention : présente sur les serveurs autonomes, de Harvester et de DSA
- nsas : présente sur le serveur CA Anomaly Detector (serveur autonome, console NFA ou serveur distinct)

La vérification des tables volumineuses de base de données peut être lente. Si vous exécutez le contrôle sur l'intégralité d'une base de données, chaque table de la base de données est verrouillée de façon séquentielle sur l'état En lecture seule. La table qui est vérifiée n'est donc pas disponible pour des opérations d'écriture.

Vous pouvez exécuter mysqlcheck sans arrêter MySQL : le processus de démon MySQL (mysqld) peut continuer de s'exécuter sur des serveurs Linux et le service MySQL peut continuer de s'exécuter sur des serveurs Windows.

Procédez comme suit :

1. Connectez-vous à un des serveurs CA Network Flow Analysis en tant qu'utilisateur avec des droits d'administrateur. Sur un serveur de Harvester Linux, connectez-vous en tant qu'utilisateur root.

2. Vérifiez les bases de données suivantes :

   - Serveur autonome : bases de données harvester, reporter, poller et data_retention
   - Serveur de Harvester (déploiement distribué) : bases de données harvester, poller et data_retention
   - Serveur de console NFA (déploiement distribué) : base de données reporter
   - Serveur de DSA (déploiement distribué) : base de données nqrptr
   - Serveur CA Anomaly Detector : base de données nsas (si CA Anomaly Detector est installé sur le serveur autonome ou sur le serveur de la console NFA

3. Entrez une des commandes mysqlcheck suivantes dans une invite de commande ou de shell :

   - Pour vérifier les tables de toutes les bases de données applicables sur le serveur :

     ```
     mysqlcheck --all-databases
     ```

   - Pour vérifier toutes les tables dans une base de données unique :

     ```
     mysqlcheck --databases db_name
     ```

     Exemple :

     ```
     mysqlcheck --databases reporter
     ```

   où :

   db_name = nom de la base de données que vous voulez vérifier

   Vous n'êtes pas obligé de spécifier le chemin de la base de données. La commande mysqlcheck trouvera automatiquement la ou les bases de données qui utilisent le port par défaut (port 3308). Le moteur de stockage personnalisé ne prend pas en charge l'utilisation de la commande mysqlcheck pour ses bases de données archive et archive15. L'exécution de la commande échoue même si vous spécifiez le port correct (port 3307) pour la connexion à ces bases de données.

   La commande vérifie chaque table, tente de réparer tout problème, puis analyse et optimise la table. La commande renvoie une liste des tables de base de données qui ont été vérifiées et signale le statut de chaque table.

Si la vérification de la table ne détecte aucune erreur, OK apparaît à côté du nom de la table. Si un avertissement est renvoyé alors que OK apparaît, le problème a été résolu. En cas d'erreurs non résolues, contactez le service de support de CA.

Etape suivante : arrêtez les services, puis sauvegardez les bases de données, décrites dans les rubriques suivantes.

Arrêt des services

Avant de sauvegarder les bases de données et de mettre à niveau le logiciel CA Network Flow Analysis, empêchez l'envoi de nouvelles données vers la console NFA tant que la mise à niveau n'est pas terminée. Si vous n'arrêtez pas les services, la mise à niveau se terminera quand même, mais certaines données collectées ne seront pas traitées.

Arrêt des services sur des serveurs Windows

Pour préparer la sauvegarde de bases de données, arrêtez les services sur tous les serveurs Windows dans le déploiement de CA Network Flow Analysis.

Procédez comme suit :

1. Connectez-vous en tant qu'utilisateur possédant des droits d'administration au niveau de CA Network Flow Analysis.
2. Ouvrez la fenêtre Services : cliquez sur Démarrer, Panneau de configuration, Outils d'administration, Services.
3. Arrêtez le service Harvester de CA NFA sur chaque serveur de Harvester.
4. Patientez 15 minutes jusqu'à la fin du traitement des fichier de données.
5. Arrêtez les autres services CA Network Flow Analysis sur chaque serveur Windows :

Service	Autonome	Harvester	Console	DSA	Anomaly Detector
Services Web de collecte et d'interrogation de CA NFA	Oui	Oui			
Conservation de données CA NFA	Oui	Oui		Oui	
Proxys DNS/SNMP de CA NFA	Oui	Oui			
CA NFA DSALoader				Oui	
Serveur de fichiers CA NFA	Oui	Oui			

Service	Autonome	Harvester	Console	DSA	Anomaly Detector
Harvester CA NFA	Oui	Oui			
Service de solveur de noms d'hôte CA NFA*					Oui*
Service de suivi CA NFA*					Oui*
Interrogateur de CA NFA	Oui	Oui			
Service de pompage CA NFA				Oui	
Reaper de CA NFA	Oui	Oui			
Source de la base d'informations de génération de rapports de CA NFA	Oui		Oui		
NetQoS MySql	Oui	Oui	Oui	Oui	
NetQoS NQMySql	Oui	Oui		Oui	
Service de gestionnaire de NetQoS Reporter	Oui		Oui		
Services généraux de NetQoS Reporter/Analyzer	Oui		Oui		
Service de pompage de NetQoS Reporter/Analyzer	Oui		Oui		
Services de requête NetQoS Reporter/Analyzer	Oui		Oui		
Outil de surveillance de NetQoS Reporter/Analyzer	Oui		Oui		
Service de rapport de NetQoS ReporterAnalyzer	Oui		Oui		

*Si CA Anomaly Detector est installé sur le serveur CA Network Flow Analysis autonome ou sur le serveur de la console NFA, arrêtez ces services CA Anomaly Detector.

Les services et la collecte de données s'arrêtent. Les fichiers de données sont traités en 15 minutes.

6. Vérifiez le répertoire suivant sur le serveur de la console NFA :

   <chemin_installation>\Netflow\datafiles\HarvesterWork

   Lorsque le dossier HarvesterWork est vide, vous pouvez sauvegarder la base de données.

   Les services sont redémarrés automatiquement pendant le processus de mise à niveau.

Arrêt des services sur des serveurs Linux

Pour préparer le système pour la sauvegarde de base de données, arrêtez les services sur tous les serveurs de Harvester Linux inclus dans le déploiement du produit.

Procédez comme suit :

1. Connectez-vous en tant que root ou avec un compte d'utilisateur sudo.
2. Arrêtez le service nfa_harvester (Harvester de CA NFA) sur chaque serveur de Harvester Linux.
3. Patientez 15 minutes jusqu'à la fin du traitement des fichier de données.
4. Arrêtez les services suivants sur le serveur du Harvester Linux.
   - mysql (NetQoS MySQL)
   - nfa_collpollws (services Web de collecte et d'interrogation de CA NFA)
   - nfa_dataretention (conservation des données CA NFA)
   - nfa_filewebservice (serveur de fichiers CA NFA)
   - nfa_mysqlCSE (moteur de stockage personnalisé NetQoS NQMySql)
   - nfa_poller (interrogateur CA NFA)
   - nfa_proxies (proxys DNS/SNMP CA NFA)
   - nfa_reaper (Reaper CA NFA)

   Après avoir arrêté les services, les fichiers Time BIN (.tbn) sont collectés et traités en 15 minutes.
5. Localisez le répertoire suivant sur le serveur de la console NFA : <chemin_installation>\Netflow\datafiles\HarvesterWork.

   Lorsque le dossier HarvesterWork est vide, vous pouvez sauvegarder la base de données.

   Les services sont redémarrés automatiquement pendant le processus de mise à niveau.

Sauvegarde des bases de données et redémarrage des services

Avant de procéder à la mise à niveau, sauvegardez les bases de données et les fichiers indiqués dans le tableau ci-dessous.

Important :

- Vous devez exécuter les sauvegardes simultanément. Des problèmes peuvent en résulter si vous restaurez des données à partir de sauvegardes dont les horodatages sont différents. Vérifiez que vos fichiers de données sauvegardés indiquent la même heure.
- Stockez les sauvegardes à un emplacement distant pour pouvoir les récupérer en cas de panne de matériel ou de système d'exploitation sur le serveur principal. Par exemple, sauvegardez les bases de données sur un partage administratif ou un lecteur réseau mappé.

Base de données	Autonome	Harvester (distribué)	Console NFA (distribué)	Serveur de DSA (distribué)	Anomaly Detector
reporter : données de présentation de l'entreprise et de configuration de la console NFA	Important		Important		
harvester : données de configuration de Harvester	Important	Important			
nqrptr : données de configuration de la collecte des données historiques (15 minutes)				Important	
nsas : données de configuration d'Anomaly Detector					Important
poller : données de configuration de l'interrogateur	Important	Important			
ReaperArchive15 : données historiques (15 minutes)	Recommandé	Recommandé		Recommandé	
Fichiers personnalisés : fichiers de configuration ou autres fichiers personnalisés	Important	Important	Important	Important	

Base de données	Autonome	Harvester (distribué)	Console NFA (distribué)	Serveur de DSA (distribué)	Anomaly Detector
data_retention personnalisée : paramètres de contrôle de la conservation de données	Important si personnalisé	Important si personnalisé		Important si personnalisé	
ReaperArchive : données en temps réel (1 minute)	Facultatif, rarement sauvegardé	Facultatif, rarement sauvegardé			

La liste suivante décrit les bases de données et leurs emplacements :

- reporter : sauvegardez les données de présentation de l'entreprise, les paramètres de configuration de la console NFA et les informations de synchronisation des dernières 24 heures.

  Chemin : répertoire <chemin_installation>\MySql\data\reporter

- harvester : sauvegardez les données de configuration du Harvester.

  Chemin : répertoire <chemin_installation>\MySql\data\harvester

- nqrptr : sauvegardez les données de configuration pour la collecte des données historiques (de résolution en 15 minutes) sur les serveurs de DSA dans un déploiement à trois niveaux.

  Chemin : <chemin_installation>\MySql\data\nqrptr

- nsas : si CA Anomaly Detector est installé sur le même serveur que la console NFA ou que le serveur autonome, sauvegardez les données de configuration pour l'instance CA Anomaly Detector en cours d'exécution. Si CA Anomaly Detector se trouve sur son propre serveur, vous pouvez effectuer cette sauvegarde lors de la mise à niveau de CA Anomaly Detector.

  Chemin : <chemin_installation>\MySql\data\nsas

- poller : sauvegardez les données de configuration de l'interrogateur. Les données de configuration de l'interrogateur et du Harvester sont essentielles pour effectuer le mappage relationnel fournissant l'accès aux données de résolution en 15 minutes. Les données de configuration de l'interrogateur fournissent des informations concernant les unités et les interfaces pour activer l'interrogation, telles que les ID persistants pour les interfaces.

  Chemin : <chemin_installation>\MySql\data\poller

- ReaperArchive15 : (facultatif) sauvegardez les données historiques (15 minutes) stockées pour les routeurs et les interfaces de génération de rapports. Cette sauvegarde est facultative, mais de nombreux administrateurs sauvegardent les données de résolution en 15 minutes.

  Chemin : <chemin_installation>\Netflow\datafiles\ReaperArchive15

- Fichiers de configuration personnalisés : sauvegardez les fichiers de configuration personnalisés (fichiers personnalisés par vous ou par le service de support de CA). Sauvegardez également toute personnalisation apportée au site Web ou aux rapports.

  Les fichiers de configuration CA Network Flow Analysis portent généralement l'extension .config, conf. ou .ini et se trouvent à l'emplacement d'installation du produit. D'autres personnalisations peuvent inclure des fichiers .css et des logos de rapport.

- ReaperArchive : (recommandé) sauvegardez les données historiques (15 minutes).

  Chemin : <chemin_installation>\Netflow\datafiles\ReaperArchive

- data_retention personnalisée : si vous avez personnalisé les paramètres de conservation des données, sauvegardez les données de configuration de conservation des données. Les paramètres de conservation de données ne sont généralement pas personnalisés, sauf avec l'aide du support Cde A. Les modifications apportées aux paramètres de conservation des données peuvent créer des problèmes, lorsque l'espace du lecteur utilisé augmente.

  Chemin : <chemin_installation>\MySql\data\data_retention

Procédez comme suit :

1. Connectez-vous en tant qu'utilisateur possédant des droits d'administration au niveau de CA Network Flow Analysis.
2. Connectez-vous au serveur :
   a. Ouvrez une session de bureau à distance.
   b. Lancez une session de connexion aux services Terminal Server ou VNC pour le serveur d'installation.
3. Copiez tous les répertoires et fichiers cibles dans un emplacement distant.
4. Redémarrez les services (page 43).

Chapitre 6: Installation du logiciel

Ce chapitre traite des sujets suivants :

Mise à niveau d'un serveur autonome

Un *déploiement autonome* comprend un serveur unique qui héberge tous les composants (le Harvester et la console NFA). Effectuez les opérations indiquées dans cette rubrique pour mettre à niveau la console NFA et le Harvester sur un serveur ou une machine virtuelle Windows uniques.

Remarque : Le programme effectue plusieurs vérifications lors de l'installation ou de la mise à niveau afin de détecter d'éventuelles erreurs au niveau du serveur. Un message d'erreur apparaît (page 81)si un problème est détecté. En cas de problème critique, le programme se ferme. Un message d'avertissement s'ouvre pour des problèmes non critiques qui peuvent être résolus à tout moment. Les éléments requis sont vérifiés afin de rechercher d'éventuels problèmes, mais vous ne recevrez pas d'avertissements pour tous les problèmes. Vous êtes responsable de la préparation du serveur et de la mise en place de toutes les étapes requises après l'installation.

Procédez comme suit pour terminer la phase relative au Harvester :

1. Vérifiez que le serveur est prêt pour la mise à niveau et qu'il remplit les conditions indiquées dans la rubrique Respect des conditions par les serveurs Windows (page 21).
2. Connectez-vous au serveur en tant qu'utilisateur membre du groupe Administrateurs.
3. Arrêtez le service de pompage sur le serveur de la console NFA :
    a. Cliquez sur Démarrer, Programmes, Outils d'administration, Services.
    b. Cliquez avec le bouton droit de la souris sur le service de pompage NetQoS Reporter/Analyzer.
    c. Sélectionnez Arrêter dans le menu contextuel.

        Le service s'arrête.
4. Connectez-vous au serveur de Harvester en tant qu'utilisateur membre du groupe Administrateurs.

5. Commencez la phase de la mise à niveau relative au Harvester : double-cliquez sur le fichier NFHarvesterSetup9.3.0.exe. Si vous ne disposez pas de ce fichier, téléchargez-le depuis le serveur (page 12).

   La fenêtre de sélection de langue s'ouvre.

6. Vérifiez que la langue appropriée est sélectionnée, puis cliquez sur OK.

   La fenêtre de Bienvenue s'affiche.

7. Cliquez sur Suivant.

   La fenêtre Contrat de licence du Harvester de CA NFA s'ouvre.

8. Lisez et acceptez les termes du contrat de licence :

   a. Lisez le contrat de licence et faites-le défiler jusqu'en bas.

   b. Si vous voulez poursuivre, cliquez sur l'option permettant d'accepter les conditions du contrat de licence. Pour activer cette option, faites défiler le texte jusqu'en bas.

   c. Cliquez sur Suivant.

      Les tests de vérification des éléments requis recherchent les éventuels problèmes et peuvent entraîner l'apparition d'un message d'erreur.

9. Si le message Avertissement de vérification des éléments requis s'affiche, lisez-le, apportez les modifications nécessaires ou notez les problèmes non critiques, puis cliquez sur OK.

   Le message Mise à niveau de la version installée apparaît et la fenêtre Sélectionner le dossier d'installation s'ouvre. Cette fenêtre affiche le chemin d'installation racine d'origine comme paramètre par défaut.

10. Vérifiez que le répertoire d'installation spécifié est correct, puis cliquez sur Suivant.

    Important : Vous devez utiliser le chemin d'installation d'origine, sinon le logiciel mis à niveau ne s'exécutera pas correctement.

    Si le programme ne trouve pas certains répertoires dans l'emplacement d'installation, un message d'erreur apparaît et la mise à niveau s'interrompt. Ce problème ne se produit pas lorsque l'installation précédente du logiciel est complètement fonctionnelle.

    La fenêtre Récapitulatif de la pré-installation s'ouvre.

11. Révisez les informations de pré-installation, puis cliquez sur Installer.

    La fenêtre d'installation du Harvester s'ouvre. A l'issue de la mise à niveau du Harvester, la fenêtre Fin de l'installation s'ouvre et signale toute erreur éventuelle.

12. (Facultatif) Si une erreur se produit lors de la mise à niveau, consultez les journaux suivants pour obtenir plus d'informations :

    - Journal d'installation général : <chemin_installation>\Harvester_Install_<horodatage>.log (où <horodatage> correspond à l'heure de création du journal)
    - Journal de migration de mise à niveau : <chemin_installation>/migrator.log

13. Dans la fenêtre Fin de l'installation, cliquez sur Terminé.

    Le programme de mise à niveau du Harvester se ferme.

Procédez comme suit pour terminer la phase relative à la console NFA :

1. Lancez le logiciel de mise à niveau de la console NFA : double-cliquez sur le fichier RAConsoleSetup9.3.0.exe dans l'explorateur Windows. Si vous ne disposez pas de ce fichier, téléchargez-le depuis le serveur (page 12).

   Le programme démarre et la fenêtre de sélection de langue s'ouvre.

2. Vérifiez que la langue appropriée est sélectionnée, puis cliquez sur OK.

   La fenêtre de Bienvenue s'affiche.

3. Cliquez sur Suivant.

   La fenêtre Contrat de licence de la console NFA s'ouvre.

4. Lisez et acceptez le contrat de licence :

   a. Lisez le contrat de licence de la console NFA et faites-le défiler jusqu'en bas.

   b. Si vous voulez poursuivre, cliquez sur l'option permettant d'accepter les conditions du contrat de licence. L'option est activée lorsque vous faites défiler l'écran jusqu'au bas du contrat.

   c. Cliquez sur Suivant.

      La fenêtre du contrat de licence tiers s'ouvre.

   d. Lisez le contrat de licence tiers et faites-le défiler jusqu'en bas.

   e. Si vous voulez poursuivre, cliquez sur l'option permettant d'accepter les conditions du contrat de licence tiers. Pour activer cette option, faites défiler le texte jusqu'en bas.

   f. Cliquez sur Suivant.

5. Si le message Avertissement de vérification des éléments requis s'affiche, lisez-le, apportez les modifications nécessaires ou notez les problèmes non critiques, puis cliquez sur OK.

   La fenêtre Confirmation de regroupement s'affiche et vous devez confirmer que vous souhaitez procéder à un déploiement autonome.

6. Vérifiez les informations saisies, puis cliquez sur OK.

   La fenêtre Récapitulatif de la pré-installation s'ouvre.

7. Révisez les informations de pré-installation, puis cliquez sur Installer.

   La fenêtre d'installation de NFA s'ouvre. A l'issue de la mise à niveau de la console NFA, la fenêtre Fin de l'installation s'ouvre.

8. Fermez le programme de mise à niveau :

   a. Sélectionnez une option de redémarrage :

      - Yes, restart my system : le système redémarre dès que vous cliquez sur Terminé.
      - No, I will restart my system myself : différez le redémarrage et effectuez-le manuellement.

   b. Cliquez sur Terminé.

      Le programme de mise à niveau se ferme. Si vous avez sélectionné l'option de redémarrage immédiat, le système redémarre et la mise à niveau se termine.

9. (Facultatif) Reportez-vous à l'historique des révisions pour vérifier que le logiciel a été mis à niveau vers la version appropriée :

   a. Ouvrez une invite de commande.

   b. Démarrez MySQL à l'aide de la commande suivante :

      ```
      mysql
      ```

   c. Affichez l'historique des révisions à l'aide de la commande suivante :

      ```
      select * from revision_history
      ```

Ensuite, effectuez les tâches postérieures à la mise à niveau (page 65).

Remarque : Si vous interrompez et redémarrez la mise à niveau, la mise à niveau reprend à partir de la dernière modification enregistrée.

Mise à niveau d'un déploiement distribué

Dans un déploiement distribué, les composants CA Network Flow Analysis sont distribués sur plusieurs serveurs. Les rubriques de cette section décrivent la procédure de mise à niveau de chaque serveur de composant.

Pour mettre à niveau un déploiement distribué à deux niveaux, suivez les procédures suivantes :

- Mise à niveau du Harvester sur un serveur Windows (page 54)
- Mise à niveau du Harvester sur un serveur Linux (page 56)
- Mise à niveau de la console (page 62)

Pour mettre à niveau un déploiement distribué à trois niveaux, suivez les procédures suivantes :

- Mise à niveau du Harvester sur un serveur Windows (page 54)
- Mise à niveau du serveur de DSA (page 59)
- Mise à niveau de la console (page 62)

Les étapes de ces rubriques suivent l'ordre de mise à niveau recommandé suivant : mise à niveau des Harvesters, mise à niveau des DSA (le cas échéant) et mise à niveau de la console NFA.

Si vous interrompez et redémarrez la mise à niveau, celle-ci reprend à partir de la dernière modification enregistrée.

Remarque : Le programme effectue plusieurs vérifications lors de l'installation ou de la mise à niveau afin de détecter d'éventuelles erreurs au niveau du serveur. Un message d'erreur apparaît (page 81)si un problème est détecté. En cas de problème critique, le programme se ferme. Un message d'avertissement s'ouvre pour des problèmes non critiques qui peuvent être résolus à tout moment. Les éléments requis sont vérifiés afin de rechercher d'éventuels problèmes, mais vous ne recevrez pas d'avertissements pour tous les problèmes. Vous êtes responsable de la préparation du serveur et de la mise en place de toutes les étapes requises après l'installation.

Mise à niveau du Harvester sur un serveur Windows

Dans un déploiement distribué, chaque Harvester est installé sur un serveur distinct. Pour mettre à niveau un Harvester sur une machine virtuelle ou un serveur Windows dédiés, suivez les étapes décrites dans cette rubrique. Ces étapes s'appliquent aux déploiements distribués à deux ou trois niveaux.

Procédez comme suit :

1. Vérifiez que le serveur est prêt pour la mise à niveau et qu'il remplit les conditions indiquées dans la rubrique Respect des conditions par les serveurs Windows (page 21).
2. Connectez-vous au serveur de la console NFA en tant qu'utilisateur membre du groupe Administrateurs.
3. Arrêtez le service de pompage sur le serveur de la console NFA :
    a. Cliquez sur Démarrer, Programmes, Outils d'administration, Services.
    b. Cliquez avec le bouton droit de la souris sur le service de pompage NetQoS Reporter/Analyzer.
    c. Sélectionnez Arrêter dans le menu contextuel.

       Le service s'arrête.
4. Connectez-vous au serveur de Harvester en tant qu'utilisateur membre du groupe Administrateurs.
5. Commencez la mise à niveau : dans le serveur du Harvester, double-cliquez sur le fichier NFHarvesterSetup9.3.0.exe dans l'explorateur Windows. Si vous ne possédez pas ce fichier, téléchargez-le (page 12).

   La fenêtre de sélection de la langue s'ouvre.
6. Vérifiez que la langue appropriée est sélectionnée, puis cliquez sur OK.

   Un message indiquant la présence d'une installation précédente s'ouvre.
7. Lisez le message, puis cliquez sur OK.

   La fenêtre de Bienvenue s'affiche.
8. Cliquez sur Suivant.

   La fenêtre Contrat de licence s'affiche.
9. Lisez et acceptez les termes du contrat de licence :
    a. Lisez le contrat de licence et faites-le défiler jusqu'en bas.
    b. Si vous voulez poursuivre, cliquez sur l'option permettant d'accepter les conditions du contrat de licence. Pour activer cette option, faites défiler le texte jusqu'en bas.

c. Cliquez sur Suivant.

   Les tests de vérification des éléments requis recherchent les éventuels problèmes et peuvent entraîner l'apparition d'un message d'erreur.

10. Si le message Avertissement de vérification des éléments requis s'affiche, lisez-le, apportez les modifications nécessaires ou notez les problèmes non critiques, puis cliquez sur OK.

    La fenêtre Sélectionner le dossier d'installation s'ouvre et affiche le chemin d'installation d'origine comme paramètre par défaut.

11. Vérifiez que le répertoire d'installation spécifié est correct, puis cliquez sur Suivant.

    Important : Vous devez utiliser le chemin d'installation d'origine, sinon le logiciel mis à niveau ne s'exécutera pas correctement.

    Si le programme ne trouve pas certains répertoires dans l'emplacement d'installation, un message d'erreur apparaît et la mise à niveau s'interrompt. Ce problème ne se produit pas lorsque l'installation précédente du logiciel est complètement fonctionnelle.

    La fenêtre Récapitulatif de la pré-installation s'ouvre.

12. Révisez les informations de pré-installation, puis cliquez sur Installer.

    La fenêtre d'installation du Harvester s'ouvre. A l'issue de la mise à niveau, la fenêtre Fin de l'installation s'ouvre et signale toute erreur potentielle.

13. (Facultatif) En cas d'erreurs, consultez les journaux suivants pour plus d'informations :

    ■ Journal d'installation général : <chemin_installation>/Harvester_Install_<horodatage>.log.

    ■ Journal de migration de mise à niveau : <chemin_installation>/migrator.log

14. Fermez le programme de mise à niveau :

    a. Sélectionnez une option de redémarrage :

       ■ Yes, restart my system : le système redémarre dès que vous cliquez sur Terminé.

       ■ No, I will restart my system myself : différez le redémarrage et effectuez-le manuellement.

    b. Cliquez sur Terminé.

       Le programme de mise à niveau se ferme. Si vous avez sélectionné l'option de redémarrage immédiat, le système redémarre et la mise à niveau se termine.

15. (Facultatif) Vérifiez les conditions suivantes :

    ■ Les services de Harvester sont en cours d'exécution.

    ■ Le Harvester reçoit les données.

- L'historique des révisions indique que le composant a été mis à niveau vers la version appropriée. Pour afficher l'historique des révisions, effectuez les sous-étapes suivantes :
    a. Lancez MySQL en entrant la commande suivante dans une invite de commande : mysql
    b. Affichez l'historique des révisions à l'aide de la commande suivante : select * from revision_history

Etape suivante :

- Pour mettre à niveau un autre Harvester, répétez ces étapes sur le serveur du Harvester supplémentaire.
- Pour continuer la mise à niveau d'un déploiement à deux niveaux, mettez à niveau le serveur de console (page 62).
- Pour continuer la mise à niveau d'un déploiement à trois niveaux, mettez à niveau le serveur de DSA (page 59).

Mise à niveau du Harvester sur un serveur Linux

Un déploiement distribué à deux niveaux peut inclure un ou plusieurs serveurs de Harvester Linux. Pour mettre à niveau un logiciel de Harvester sur une machine virtuelle ou un serveur Linux dédiés, effectuez les opérations indiquées dans cette rubrique.

Procédez comme suit :

1. Vérifiez que le serveur est prêt pour la mise à niveau et qu'il remplit les conditions indiquées dans la rubrique Respect des conditions par les serveurs Linux (page 37).
2. Connectez-vous au serveur de la console NFA en tant qu'utilisateur membre du groupe Administrateurs.
3. Arrêtez le service de pompage sur le serveur de la console NFA :
    a. Cliquez sur Démarrer, Programmes, Outils d'administration, Services.
    b. Cliquez avec le bouton droit de la souris sur le service de pompage NetQoS Reporter/Analyzer.
    c. Sélectionnez Arrêter dans le menu contextuel.

    Le service s'arrête.
4. Connectez-vous au serveur du Harvester en tant qu'utilisateur root.

    Vous pouvez installer le logiciel localement ou à distance, par exemple, via ssh lorsque vous êtes connecté avec des droits d'accès d'utilisateur root.

    Remarque : Si vous ne disposez pas d'un compte root, utilisez un compte disposant des droits sudo.
5. Ouvrez une invite de commande.

6. Exécutez la commande suivante pour modifier la limite des fichiers ouverts ulimit :
   `ulimit -n valeur_ulimit`

   Exemple :
   `ulimit -n 65536`

7. Préparez le fichier d'installation ou de mise à niveau pour l'exécution :

   a. Connectez-vous au serveur du Harvester en tant qu'utilisateur root.

      Vous pouvez installer ou mettre à niveau le logiciel localement ou à distance, par exemple, via ssh lorsque vous êtes connecté avec des droits d'utilisateur root. Si vous ne disposez pas d'un compte root, utilisez un compte associé à des droits sudo.

   b. Exécutez la commande chmod sur le fichier dans une fenêtre de terminal :
      `chmod u+x NFHarvesterSetup9.3.0.bin`

   c. (Facultatif) Exécutez la commande list pour vérifier que le fichier est exécutable :
      `ls -al`

      Les paramètres d'autorisations de fichiers sont affichés.

8. Exécutez le logiciel d'installation ou de mise à niveau :
   `./NFHarvesterSetup9.3.0.bin`

   La fenêtre de sélection de langue s'ouvre.

9. Vérifiez que la langue appropriée est sélectionnée, puis cliquez sur OK.

   Un message indiquant la présence d'une installation précédente s'ouvre.

10. Lisez le message, puis cliquez sur OK.

    La fenêtre de Bienvenue s'affiche.

11. Cliquez sur Suivant.

    La fenêtre Contrat de licence s'affiche.

12. Lisez et acceptez les termes du contrat de licence :

    a. Lisez le contrat de licence et faites-le défiler jusqu'en bas.

    b. Si vous voulez poursuivre, cliquez sur l'option permettant d'accepter les conditions du contrat de licence. Pour activer cette option, faites défiler le texte jusqu'en bas.

    c. Cliquez sur Suivant.

       Les tests de vérification des éléments requis recherchent les éventuels problèmes et peuvent entraîner l'apparition d'un message d'erreur.

13. Si le message Avertissement de vérification des éléments requis s'affiche, lisez-le, apportez les modifications nécessaires ou notez les problèmes non critiques, puis cliquez sur OK.

    La fenêtre Sélectionner le dossier d'installation s'ouvre. Cette fenêtre affiche le chemin d'installation racine d'origine comme paramètre par défaut.

14. Vérifiez que le répertoire d'installation spécifié est correct, puis cliquez sur Suivant.

    Important : Vous devez utiliser le chemin d'installation d'origine, sinon le logiciel mis à niveau ne s'exécutera pas correctement.

    Si le programme ne trouve pas certains répertoires dans l'emplacement d'installation, un message d'erreur apparaît et la mise à niveau s'interrompt. Ce problème ne se produit pas lorsque l'installation précédente du logiciel est complètement fonctionnelle.

    La fenêtre Récapitulatif de la pré-installation s'ouvre.

15. Révisez les informations de pré-installation, puis cliquez sur Installer.

    La fenêtre d'installation du Harvester s'ouvre. A l'issue de la mise à niveau, la fenêtre Fin de l'installation s'ouvre et signale toute erreur potentielle.

16. (Facultatif) Passez en revue les erreurs éventuelles en consultant le journal d'installation (Harvester_Install_<horodatage>.log dans le répertoire <chemin_installation>).

17. Cliquez sur Terminé.

    Le programme de mise à niveau se ferme. Le Harvester est mis à niveau et les services CA Network Flow Analysis sont lancés automatiquement.

18. (Facultatif) Vérifiez les conditions suivantes :

    - (Déploiement d'architecture à deux niveaux) Les services de Harvester sont en cours d'exécution.

    - Le Harvester reçoit les données.

    - L'historique des révisions indique que le composant a été mis à niveau vers la version appropriée. Pour afficher l'historique des révisions, effectuez les sous-étapes suivantes :

        a. Lancez MySQL en entrant la commande suivante dans une invite de commande : mysql

        b. Affichez l'historique des révisions à l'aide de la commande suivante : select * from revision_history

Etape suivante :

- Pour mettre à niveau un autre Harvester, répétez ces étapes sur le serveur du Harvester supplémentaire.
- Pour continuer la mise à niveau d'un déploiement à deux niveaux, mettez à niveau le serveur de console (page 62).
- Pour continuer la mise à niveau d'un déploiement à trois niveaux, mettez à niveau le serveur de DSA (page 59).

Mise à niveau de DSA dans un déploiement distribué à trois niveaux

Dans un déploiement distribué à trois niveaux, chaque DSA est installée sur un serveur distinct. Effectuez la procédure mentionnée dans cette rubrique pour mettre à niveau une console DSA sur un serveur ou une machine virtuelle Windows dédiés.

Remarque : Si vous utilisez un DSA Linux, contactez votre responsable du support CA désigné ou l'équipe de ventes chargée de votre compte pour obtenir des informations sur un DSA Windows.

Procédez comme suit :

1. Assurez-vous que le serveur d'installation répond à la configuration requise suivante :
   - Le serveur est prêt pour la mise à niveau et il remplit les conditions indiquées dans la rubrique Respect des conditions par les serveurs Windows (page 21).
   - Les serveurs de Harvester ont été mis à niveau (page 54).
2. Vérifiez que le traitement des données collectées par le DSA est terminé :
   a. Connectez-vous au serveur de la console NFA avec un compte disposant des droits d'administrateur de CA Network Flow Analysis.
   b. Sur le serveur de la console NFA, recherchez le répertoire suivant : <chemin_installation>/Reporter/datashare/data/<adresse_IP_serveur_DSA>.
   c. Vérifiez que le répertoire ne contient aucun fichier CSV. Si des fichiers CSV sont présents, vérifiez jusqu'à ce que les fichiers disparaissent. Les fichiers seront traités et disparaîtront dans un délai de 15 minutes.
3. Connectez-vous au serveur de DSA en tant qu'utilisateur membre du groupe Administrateurs.
4. Commencez la mise à niveau : double-cliquez sur le fichier DSASetup9.3.0.exe dans l'explorateur Windows.

   La fenêtre de sélection de langue s'ouvre.
5. Vérifiez que la langue appropriée est sélectionnée, puis cliquez sur OK.

   La fenêtre Contrat de licence s'affiche.

6. Lisez et acceptez les termes du contrat de licence :

   a. Lisez le contrat de licence et faites-le défiler jusqu'en bas.

   b. Si vous voulez poursuivre, cliquez sur l'option permettant d'accepter les conditions du contrat de licence. Pour activer cette option, faites défiler le texte jusqu'en bas.

   c. Cliquez sur Suivant.

      Les tests de vérification des éléments requis recherchent les éventuels problèmes et peuvent entraîner l'apparition d'un message d'erreur.

7. Si le message Avertissement de vérification des éléments requis s'affiche, lisez-le, apportez les modifications nécessaires ou notez les problèmes non critiques, puis cliquez sur OK.

   La fenêtre Sélectionner le dossier d'installation s'ouvre et affiche le chemin d'installation d'origine comme paramètre par défaut.

8. Suivez les options de vérification des répertoires d'installation :

   a. Cliquez sur Suivant.

      Important : Vous devez utiliser le chemin d'installation d'origine, sinon le logiciel mis à niveau ne s'exécutera pas correctement.

      Si le programme ne trouve pas certains répertoires dans le dossier d'installation, un message d'erreur s'affiche et la mise à niveau s'interrompt. Ce problème ne se produit pas lorsque l'installation précédente du logiciel est complètement fonctionnelle.

      La fenêtre Sélectionner l'emplacement du répertoire de données MySQL s'ouvre. Elle contient le chemin d'installation d'origine du répertoire de données MySQL.

      Le message suivant apparaît : Le dossier sélectionné n'est pas vide. Vérifiez que vous avez sauvegardé le contenu du répertoire.

   b. Dans la boîte de dialogue Sélectionner l'emplacement du répertoire de données MySQL, cliquez sur Suivant.

      Important : Vous devez utiliser le chemin d'installation d'origine pour le répertoire de données MySQL.

      La fenêtre Sélectionner l'emplacement temporaire du répertoire de données MySQL s'ouvre. Elle contient le chemin d'installation d'origine du répertoire de données MySQL.

   c. Cliquez sur OK.

d. Cliquez sur Suivant.

   Important : Vous devez utiliser le chemin d'installation d'origine pour le répertoire temporaire MySQL.

   MySQL est configuré et la fenêtre Récapitulatif de la pré-installation s'ouvre.

e. Cliquez sur Suivant.

   Important : Vous devez utiliser le chemin d'installation d'origine pour le répertoire temporaire MySQL.

   MySQL est configuré et la fenêtre Récapitulatif de la pré-installation s'ouvre.

9. Révisez les informations de pré-installation, puis cliquez sur Installer.

   La fenêtre d'installation de DSA s'ouvre. A l'issue de la mise à niveau, la fenêtre Fin de l'installation s'ouvre et signale toute erreur éventuelle.

10. Cliquez sur Terminé.

    Le programme de mise à niveau se ferme. Le DSA est mis à niveau et les services de DSA sont redémarrés.

11. (Facultatif) Vérifiez les conditions suivantes :

    ■ Les services DSA sont en cours d'exécution.

    ■ Le DSA reçoit les données.

    ■ L'historique des révisions indique que le composant a été mis à niveau vers la version appropriée. Pour afficher l'historique des révisions, effectuez les sous-étapes suivantes :

      a. Lancez MySQL en entrant la commande suivante dans une invite de commande : mysql

      b. Affichez l'historique des révisions à l'aide de la commande suivante : select * from revision_history

12. (Facultatif) Vérifier le journal DSA_Install_<horodatage> régulièrement. Ce journal se trouve dans le répertoire racine à l'emplacement d'installation (par exemple, dans le répertoire \\CA\NFA). Utilisez le journal pour surveiller la migration des tables de bases de données de DSA vers le nouveau format.

    La migration des données de table de base de données DSA commence dès que le service CA NFA DSALoader redémarre. Le journal DSA_Install répertorie les tables dès leur migration. Neuf tables sont migrées pour chaque agent ou interface. Si vous disposez d'un grand nombre d'agents et de nombreuses données stockées, la migration peut être prolongée.

Etape suivante :

■ Pour mettre à niveau un DSA supplémentaire sur un autre serveur, effectuez de nouveau ces étapes.

■ Pour mettre à niveau le serveur de console (page 62), consultez la rubrique suivante.

Mise à niveau de la console NFA

Les déploiements distribués utilisent différents serveurs pour la console NFA, les Harvesters et les DSA du déploiement. Effectuez les opérations indiquées dans cette rubrique pour mettre à niveau la console NFA sur un serveur ou une machine virtuelle Windows dédiés.

Procédez comme suit :

1. Assurez-vous que le serveur répond à la configuration requise suivante :
   - Le serveur est prêt pour la mise à niveau et il remplit les conditions indiquées dans la rubrique Respect des conditions par les serveurs Windows (page 21).
   - Les serveurs de Harvester ont été mis à niveau (page 54).
   - Si vous utilisez un déploiement d'architecture à trois niveaux, les serveurs de DSA sont mis à niveau (page 59).
2. Connectez-vous au serveur de la console NFA en tant qu'utilisateur avec des droits d'administrateur pour le système et CA Network Flow Analysis.
3. (Architecture à trois niveaux uniquement) Vérifiez que les DSA ont récupéré toutes les données de type 15 minutes à partir du serveur de la console NFA :
   a. Sur le serveur de la console NFA, recherchez le répertoire suivant : <chemin_installation>/Reporter/datashare/data/<adresse_IP_serveur_DSA>.
   b. Vérifiez que le répertoire ne contient aucun fichier CSV. Si des fichiers CSV sont présents, attendez que les fichiers disparaissent. Suite à l'arrêt du service de pompage, les fichiers CSV doivent disparaître dans un délai de 15 minutes.
4. Commencez la mise à niveau : dans le serveur de la console NFA, double-cliquez sur le fichier RAConsoleSetup9.3.0.exe dans l'explorateur Windows.

   La fenêtre de sélection de langue s'ouvre.
5. Vérifiez que la langue appropriée est sélectionnée, puis cliquez sur OK.

   La fenêtre de Bienvenue s'affiche.
6. Cliquez sur Suivant.

   La fenêtre Contrat de licence s'affiche.
7. Lisez et acceptez le contrat de licence :
   a. Lisez le contrat de licence de la console NFA et faites-le défiler jusqu'en bas.
   b. Si vous voulez poursuivre, cliquez sur l'option permettant d'accepter les conditions du contrat de licence. L'option est activée lorsque vous faites défiler l'écran jusqu'au bas du contrat.
   c. Cliquez sur Suivant.

      La fenêtre du contrat de licence tiers s'ouvre.

   d. Lisez le contrat de licence tiers et faites-le défiler jusqu'en bas.
   e. Si vous voulez poursuivre, cliquez sur l'option permettant d'accepter les conditions du contrat de licence tiers. Pour activer cette option, faites défiler le texte jusqu'en bas.
   f. Cliquez sur Suivant.

8. Si le message Avertissement de vérification des éléments requis s'ouvre, révisez les résultats du test :
   a. Corrigez les problèmes immédiatement ou patientez jusqu'à la fin de l'exécution du programme de mise à niveau. Pour plus d'informations sur ces avertissements, reportez-vous à la rubrique Dépannage (page 81).
   b. Cliquez sur OK.

      Le message Mise à niveau de la version installée s'ouvre.

9. Passez en revue les informations :
   a. Vérifiez que les informations existantes sur la version après mise à niveau sont correctes, puis cliquez sur OK.

      Le message s'ouvre de nouveau et indique le chemin d'installation racine. Le programme de mise à niveau utilise toujours le chemin d'origine, qui est C:\CA\NFA par défaut.

   b. Passez en revue les informations de chemin, puis cliquez sur OK.

      La fenêtre Sélectionner le dossier d'installation s'ouvre.

10. (Facultatif) Lorsque vous y êtes invité, cliquez sur Sélectionner pour modifier l'emplacement d'installation du programme ou entrez le nouveau chemin d'accès manuellement.

    L'emplacement par défaut est C:\CA\NFA. Utilisez le même chemin d'installation pour les serveurs de Harvester et de console NFA. Nous vous recommandons d'installer les composants CA Network Flow Analysis sur un lecteur non système.

    La fenêtre Récapitulatif de la pré-installation s'ouvre.

11. Révisez les informations, puis cliquez sur Installer.

    La fenêtre d'installation de NFA s'ouvre. A l'issue de la mise à niveau, la fenêtre Fin de l'installation s'ouvre et signale toute erreur éventuelle.

12. (Facultatif) En cas d'erreur, consultez le journal d'installation à l'emplacement suivant : <chemin_installation>/NFA_Install_<horodatage>.log.

13. Fermez le programme de mise à niveau :

    a. Sélectionnez une option de redémarrage :

       - Yes, restart my system : le système redémarre dès que vous cliquez sur Terminé.

       - No, I will restart my system myself : différez le redémarrage et effectuez-le manuellement.

    b. Cliquez sur Terminé.

       Le programme de mise à niveau se ferme. Si vous avez sélectionné l'option de redémarrage immédiat, le système redémarre et la mise à niveau se termine.

14. (Facultatif) Reportez-vous à l'historique des révisions pour vérifier que le logiciel a été mis à niveau vers la version appropriée :

    a. Ouvrez une invite de commande.

    b. Démarrez MySQL à l'aide de la commande suivante :

       ```
       mysql
       ```

    c. Affichez l'historique des révisions à l'aide de la commande suivante :

       ```
       select * from revision_history
       ```

Ensuite, effectuez les tâches postérieures à la mise à niveau (page 65).

Chapitre 7: Tâches postérieures à la mise à niveau

Effectuez les tâches postérieures à l'installation suivantes :

- Configurez SNMP sur tous les Harvesters Linux inclus dans votre déploiement. (page 67)
- Excluez les répertoires suivants des analyses en temps réel : C:\Windows\Temp et <chemin_installation> et tous leurs sous-répertoires. Les analyses en temps réel de ces répertoires peuvent endommager la base de données.
- N'implémentez pas la compression de l'espace disque. La compression d'espace disque peut endommager la base de données et détériorer les performances système.
- Nous vous recommandons d'installer Adobe Flash Player sur les systèmes équipés d'ordinateurs de bureau ayant accès à la console NFA et d'installer Adobe Reader sur les systèmes équipés d'ordinateurs de bureau ayant accès à la documentation au format PDF.

<table>
<tr><th>Serveur autonome</th><th>Serveur de console NFA distribué</th><th>Serveur de Harvester distribué (Windows)</th><th>Distribution à 3 niveaux Serveur DSA</th></tr>
<tr><td colspan="4">■ Synchronisation de l'heure système (page 68)</td></tr>
<tr><td colspan="2">■ (Recommandé) Mise jour de la liste des sites Internet approuvés (page 69) *</td><td colspan="2"></td></tr>
<tr><td>■ (Recommandé) Modification des listes ACL de routeur (page 70)</td><td></td><td>■ (Recommandé) Modification des listes ACL de routeur (page 70) **</td><td></td></tr>
<tr><td colspan="2">■ (Recommandé) Désactivation du contrôle de compte d'utilisateur (page 70)</td><td colspan="2"></td></tr>
<tr><td colspan="2">■ (Recommandé) Configuration de l'expiration du contenu Web (page 71)</td><td colspan="2"></td></tr>
<tr><td colspan="4">■ (Recommandé) Ajout d'une clé pour empêcher les faux positifs SNMP (page 72)</td></tr>
<tr><td colspan="4">■ (Facultatif) Configuration de la corbeille (page 72)</td></tr>
<tr><td colspan="4">■ (Facultatif) Désactivation des services non requis (page 73)</td></tr>
</table>

*Vérifiez que cette tâche a également été réalisée sur les systèmes qui accèdent à la console NFA.

** Dans un déploiement distribué, vérifiez que les listes de contrôle d'accès du routeur sont configurées pour autoriser les Harvesters à effectuer une interrogation SNMP.

Ce chapitre traite des sujets suivants :

Mise à niveau et vérification de Performance Center

Assurez-vous que la console NFA ou le serveur autonome sont enregistrés comme source de données pour l'un des produits suivants :

- CA Performance Center 2.4/2.3 ou
- CA NetQoS Performance Center 6.1.205 SP2/6.1.194

Si vous devez mettre à niveau CA Performance Center, procédez à cette opération maintenant. Pour plus d'instructions, consultez le *Manuel d'installation de CA Performance Center*.

Certains liens de fonction de la page Administration sont activés uniquement après l'enregistrement de CA Network Flow Analysis comme source de données. Pour obtenir les instructions à suivre pour l'enregistrement, consultez la rubrique Enregistrement de CA Network Flow Analysis dans le *Manuel de l'administrateur de CA Network Flow Analysis*. Une fois l'enregistrement terminé, examinez les résultats dans les consoles Performance Center et NFA. Effectuez les modifications nécessaires.

Configuration du protocole SNMP sur les serveurs Linux

Pour configurer un serveur Linux pour un Harvester, effectuez les tâches suivantes :

- Configurez le fichier de configuration Net-SNMP.
- Configurez SNMP pour qu'il se lance automatiquement lors du démarrage.
- Lancez le service snmpd.

Requis/facultatif	Serveurs à configurer
Obligatoire	Harvesters Linux

Procédez comme suit :

1. Connectez-vous en tant que root et ouvrez une invite shell.
2. (Extrêmement recommandé) Procédez comme suit pour installer le fichier de configuration Net-SNMP. Ce fichier de configuration est requis pour l'interrogation SNMP de l'outil de surveillance.

   Remarque : Si vous avez un fichier de configuration snmp personnalisé et non un fichier par défaut sous /etc/snmp/snmp.conf, vous pouvez ignorer cette étape et mettre à jour votre fichier de configuration existant à la place. Dans ce cas, consultez un administrateur pour mettre à jour les paramètres requis afin qu'ils correspondent aux paramètres de l'exemple de fichier de configuration. Par exemple, vérifiez que la valeur de rocommunity est définie comme dans l'exemple de fichier de configuration.

   Si vous utilisez un nom de communauté personnalisé comme valeur rocommunity, utilisez-le tout au long du déploiement de CA Network Flow Analysis :

   – Fichier snmpd.conf sur chaque serveur de Harvester Linux

   – Service SNMP sur chaque serveur Windows

   – Page de paramètres de l'outil de surveillance de la console NFA

   a. (Recommandé) Sauvegardez le fichier de configuration dans le répertoire /etc, par exemple en saisissant la commande suivante :
   ```
   cp /etc/snmp/snmpd.conf /etc/snmp/snmpd.conf.bak
   ```

   b. Accédez au répertoire Netflow :
   ```
   cd <répertoire_installation>/Netflow
   ```
   où <répertoire_installation> correspond au répertoire cible utilisé pour l'installation du Harvester (/opt/CA/NFA/ ou un emplacement personnalisé).

   c. Copiez le fichier snmpd.conf présent dans le répertoire Netflow et collez-le dans le répertoire /etc/snmp (écrasez le fichier existant) :
   ```
   cp -i snmpd.conf /etc/snmp
   ```

   d. Confirmez le remplacement lorsque vous y êtes invité.

e. Vérifiez que le fichier de configuration est en place :
```
ls -l /etc/snmp/snmpd.conf
```

f. Vérifiez que le fichier de configuration dispose des autorisations appropriées :
```
chmod 600 snmpd.conf
```

3. Configurez le service SNMP pour qu'il se lance automatiquement à chaque démarrage en entrant la commande suivante :
```
chkconfig snmpd on
```

4. Démarrez le service SNMP de l'une des manières suivantes :

   ■ Entrez la commande :
   ```
   service snmpd start
   ```

   ■ Accédez aux services dans l'interface utilisateur, sélectionnez snmpd, Démarrer, puis cliquez sur Enregistrer.

   Le service SNMP commence par le nom de communauté défini dans le fichier snmpd.

Synchronisation de l'heure système

Synchronisez l'heure système sur tous les serveurs dotés de composants CA Network Flow Analysis, sauf si l'heure système est synchronisée automatiquement. Nous vous recommandons également de synchroniser l'heure système de tous les serveurs Linux de votre déploiement, y compris celle du serveur qui héberge CA Performance Center.

Requis/facultatif	Serveurs à configurer
Obligatoire	Tous les serveurs

Cette rubrique offre une approche de synchronisation de l'heure système sur les serveurs Windows Server 2008.

Procédez comme suit :

1. Connectez-vous en tant qu'utilisateur possédant des droits d'administration au niveau de CA Network Flow Analysis.
2. Cliquez avec le bouton droit de la souris sur la date ou l'heure dans la partie droite de la barre des tâches et sélectionnez Ajuster la date/l'heure.

   La boîte de dialogue Date et heure s'ouvre.
3. Cliquez sur l'onglet Temps Internet.
4. Cliquez sur Modifier les paramètres.

   La boîte de dialogue Paramètres d'heure Internet s'ouvre.
5. Activez l'option Synchroniser avec un serveur de temps Internet.

6. Sélectionnez le serveur pour la synchronisation. La valeur par défaut est time.windows.com.
7. Cliquez sur Mettre à jour maintenant.

   L'heure système est synchronisée avec le serveur sélectionné.
8. Dans la boîte de dialogue Paramètres d'heure Internet, cliquez sur OK.
9. Dans la boîte de dialogue Date et heure, cliquez sur OK.

Remarque : Si certaines unités de collecte se trouvent dans différents fuseaux horaires, définissez chaque unité en fonction du fuseau horaire local. Les heures sont converties en heures de Greenwich (GMT).

Mise à jour de la liste des sites Internet approuvés

Ajoutez le serveur de la console NFA à la liste de sites Internet fiables, sauf si vos paramètres de sécurité de navigateur permettent l'accès illimité aux sites Internet.

Remarque : Cette procédure s'applique à Internet Explorer 8, à savoir la version recommandée du navigateur.

Requis/facultatif	**Serveurs à configurer**
Recommandé	Autonome ou de console NFA

Procédez comme suit :

1. Connectez-vous en tant qu'utilisateur possédant des droits d'administration au niveau de CA Network Flow Analysis.
2. Lancez Internet Explorer sur le serveur de la console NFA.
3. Sélectionnez Outils, Options Internet.

   La boîte de dialogue Options Internet s'ouvre.
4. Sélectionnez l'onglet Sécurité.
5. Cliquez sur l'icône Sites approuvés.
6. Cliquez sur Sites.

   La boîte de dialogue Sites approuvés s'ouvre.
7. Dans le champ Ajouter ce site Web à la zone, entrez **https://localhost**.
8. Cliquez sur Ajouter.

   Votre modification est enregistrée et le site est ajouté à la liste de sites Web.

9. Quitter :
   a. Cliquez sur Fermer.
   b. Dans la boîte de dialogue Options Internet, cliquez sur OK.

      La boîte de dialogue Options Internet se ferme.

Modification des listes de contrôle d'accès

Nous vous recommandons de configurer les listes de contrôle d'accès de routeur (ACL) pour assurer que les Harvesters peuvent effectuer l'interrogation SNMP.

Requis/facultatif	Serveurs à configurer
Recommandé	Harvesters autonomes, Windows

Remarque : Si vous configurez l'exportation des flux à partir des interfaces de bouclage, vérifiez que CA Network Flow Analysis peut accéder aux adresses IP de ces interfaces.

Désactivation du contrôle de compte d'utilisateur (UAC)

Nous vous recommandons de désactiver le contrôle de compte d'utilisateur (UAC) sur les serveurs autonomes Windows et sur le serveur de la console NFA. L'option UAC n'est pas entièrement prise en charge par la version actuelle de CA Network Flow Analysis. L'activation de l'option UAC sur le serveur autonome ou sur le serveur de la console NFA peut entraîner un comportement inattendu.

Requis/facultatif	Serveurs à configurer
Recommandé	Autonome ou de console NFA

Procédez comme suit :

1. Connectez-vous en tant qu'utilisateur possédant des droits d'administration au niveau de CA Network Flow Analysis.
2. Cliquez sur Démarrer, Panneau de configuration, puis Comptes d'utilisateurs.

   La fenêtre Comptes d'utilisateurs s'ouvre.
3. Cliquez sur Modifier les paramètres de contrôle de compte d’utilisateur.

   La boîte de dialogue paramètres de contrôle de compte d’utilisateur s'ouvre.

4. Déplacez la barre de curseur vers le niveau inférieur Ne jamais notifier, le cas échéant.

   L'option UAC est définie pour être désactivée pour tous les comptes locaux sur le serveur.

5. Cliquez sur OK.

   Vous revenez à la page Comptes d'utilisateurs.

6. Fermez la fenêtre.

Configuration de l'expiration du contenu Web

Nous vous recommandons de configurer IIS pour garantir la mise à jour du contenu Web affiché. Lorsque le paramètre d'expiration immédiate du contenu Web est activé, le navigateur affiche une page mise à jour à partir du serveur plutôt qu'à partir du contenu du cache.

Requis/facultatif	Serveurs à configurer
Recommandé	Autonome ou de console NFA

Procédez comme suit :

1. Connectez-vous en tant qu'utilisateur possédant des droits d'administration au niveau de CA Network Flow Analysis.
2. Sélectionnez Démarre, Outils administratifs, Gestionnaire Internet Information Services (IIS).

   La fenêtre Gestionnaire des services Internet (IIS) s'ouvre.

3. Affichez les options d'expiration du contenu Web :

   a. Cliquez sur le nom de serveur dans le volet Connexions.

      Les fonctionnalités de serveur sont affichées.

   b. Double-cliquez sur l'icône En-têtes de réponse HTTP dans le groupe Fonctionnalités HTTP.

      La fenêtre affiche les en-têtes de réponse HTTP actuels.

   c. Dans le volet Actions, cliquez sur Définir les en-têtes communs.

      La boîte de dialogue Définir les en-têtes communs s'ouvre.

4. Sélectionnez les options suivantes :

   ■ Case à cocher Expiration du contenu

   ■ Immédiatement

5. Quitter :
    a. Cliquez sur OK pour enregistrer les modifications et fermer la boîte de dialogue.
    b. Fermez la fenêtre Gestionnaire des services Internet (IIS).

Création d'une clé TrapConfiguration

Nous vous recommandons de créer une clé TrapConfiguration vide dans le registre Windows pour empêcher la journalisation d'événements faux positifs par le service SNMP. Cette rubrique décrit la procédure à suivre.

Requis/facultatif	Serveurs à configurer
Recommandé	Tous les serveurs

Procédez comme suit :

1. Connectez-vous en tant qu'utilisateur possédant des droits d'administration au niveau de CA Network Flow Analysis.
2. Ouvrez une invite de commande.
3. Exécutez la commande suivante :

    ```
    reg add
    HKLM\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\TrapConf
    iguration
    ```

    Si la commande s'exécute avec succès, la valeur "Opération terminée" est renvoyée.

    La clé de registre TrapConfiguration est créée à l'emplacement suivant : HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters.

Configuration de la corbeille

Vous pouvez également configurer la corbeille pour supprimer immédiatement et de façon définitive les fichiers supprimés sur le serveur. Par défaut, le système enregistre des copies de fichiers supprimés dans la corbeille.

Requis/facultatif	Serveurs à configurer
Recommandé	Tous les serveurs

Procédez comme suit :

1. Connectez-vous en tant qu'utilisateur possédant des droits d'administration au niveau de CA Network Flow Analysis.
2. Sur le bureau, cliquez avec le bouton droit de la souris sur l'icône de la corbeille.
3. Sélectionnez Propriétés dans le menu.

   La boîte de dialogue Propriétés de la corbeille s'ouvre.
4. Sélectionnez Disque local (C:) dans l'onglet Général.
5. Sélectionnez Ne pas déplacer les fichiers vers la Corbeille. Supprimer immédiatement les fichiers lorsqu'ils sont effacés.
6. Cliquez sur Apply.
7. Répétez ces étapes pour chaque lecteur supplémentaire que vous voulez configurer.
8. Cliquez sur OK.

Désactivation des services Windows non requis

Vous pouvez désactiver les services dont le produit n'a pas besoin. Cette étape est conçue pour aider à sécuriser vos serveurs. Elle n'est pas obligatoire. Si les services suivants sont nécessaires pour une autre raison, ne les désactivez pas.

Si vous voulez désactiver les services non requis sur les serveurs Windows de votre déploiement, effectuez les étapes incluses dans cette rubrique.

Requis/facultatif	Serveurs à configurer
Facultatif	Tous les serveurs (Windows)

Procédez comme suit :

1. Connectez-vous en tant qu'utilisateur possédant des droits d'administration au niveau de CA Network Flow Analysis.
2. Ouvrez la fenêtre Services : cliquez sur Démarrer, Outils d'administration, Services.

   La fenêtre Services s'affiche.
3. Cliquez avec le bouton droit de la souris sur les services suivants et sélectionnez Manuel ou Désactivé.

   Ne sélectionnez pas l'option Arrêter, car elle démarre à nouveau les services lors du redémarrage du serveur.

Services Windows Server pouvant être désactivés		
■ Service de la passerelle de la couche Application	■ Gestion des applications	■ Propagation du certificat
■ Client de suivi de lien distribué	■ Distributed Transaction Coordinator	■ Client DNS
■ Publication des ressources de découverte de fonctions	■ Accès du périphérique d'interface utilisateur	■ Assistance IP
■ Découverte de la topologie de la couche de liaison	■ Service Initiateur iSCSI de Microsoft	■ Planificateur de classes multimédias
■ NetLogon	■ Service Liste des réseaux	■ Service Connaissance des emplacements réseau
■ Service Enumérateur d'appareil mobile	■ Spouleur d'impression	■ Gestionnaire de connexion automatique d'accès distant
■ Gestionnaire de connexions d'accès distant	■ Accès à distance au Registre	■ Fournisseur d'un jeu de stratégie résultant
■ Ouverture de session secondaire	■ Carte à puce	■ Stratégie de retrait de la carte à puce
■ Application d'assistance de la Console d'administration spéciale	■ Détection SSDP	■ Service Panneau de saisie Tablet PC
■ Téléphonie	■ Cliché instantané de volume	■ Audio Windows
■ Générateur de points de terminaison du service Audio Windows	■ Windows CardSpace	■ Système de couleurs Windows
■ Service de découverte automatique de Proxy Web pour les services HTTP Windows	■ Carte de performance WMI	

Chapitre 8: Désinstallation du logiciel

CA Network Flow Analysis 9.3.0 inclut une option de désinstallation du produit que vous pouvez utiliser pour supprimer CA Network Flow Analysis après une installation ou une mise à niveau.

Remarques :

- Le programme de désinstallation n'inclut aucune option permettant d'annuler l'action : une fois que vous désinstallez le logiciel, vous ne pourrez pas restaurer les fichiers supprimés automatiquement.
- Vous pouvez installer et désinstaller le logiciel CA Network Flow Analysis une fois ou deux fois sans incident. En cas de problème, contactez le site de support CA et n'effectuez pas plusieurs opérations d'installation et de désinstallation du logiciel.

Important : Si vous avez effectué une mise à niveau à partir de CA NetQoS ReporterAnalyzer 9.0.1, n'utilisez pas l'option Désinstaller.

Ce chapitre traite des sujets suivants :

Conditions de désinstallation

Avant de commencer à désinstaller le logiciel CA Network Flow Analysis sur un serveur, vérifiez que le composant fonctionne.

Vérifiez que les bases de données appropriées sont présentes, comme le décrit le tableau suivant.

Base de données	Emplacement
reporter	<chemin_installation>\MySql\data\reporter sur le serveur autonome ou sur le serveur de la console NFA
harvester	<chemin_installation>\MySql\data\harvester sur les serveurs autonomes ou de Harvester
nqrptr	<chemin_installation>\MySql\data\nqrptr sur les serveurs DSA dans un déploiement à trois niveaux
poller	<chemin_installation>\MySql\data\poller sur les serveurs autonomes ou de Harvester
ReaperArchive15	<chemin_installation>\Netflow\datafiles\ReaperArchive15 sur les serveurs autonomes ou de Harvester

Base de données	Emplacement
data_retention	<chemin_installation>\MySql\data\data_retention sur les serveurs autonomes ou de Harvester
ReaperArchive	<chemin_installation>\Netflow\datafiles\ReaperArchive sur les serveurs autonomes ou de Harvester

Vérifiez que les services CA Network Flow Analysis et MySQL s'exécutent, comme le décrit le tableau suivant :

Service	Autonome	Harvester	Console	DSA (3 niveaux)
Services Web de collecte et d'interrogation de CA NFA (nfa_collpollws sous Linux)	Oui	Oui		
Conservation de données CA NFA (nfa_dataretention sous Linux)	Oui	Oui		
Proxys DNS/SNMP de CA NFA (nfa_proxies sous Linux)	Oui	Oui	Oui	Oui
CA NFA DSALoader				Oui
Serveur de fichiers CA NFA (nfa_filewebservice sous Linux)	Oui	Oui	Oui (3 niveaux)	
Harvester CA NFA (nfa_harvester sous Linux)	Oui	Oui		
Interrogateur CA NFA (nfa_poller sous Linux)	Oui	Oui		
Service de pompage CA NFA				Oui
Reaper de CA NFA (nfa_reaper sous Linux)		Oui		
Source de la base d'informations de génération de rapports de CA NFA	Oui		Oui	
NetQoS MySql	Oui	Oui	Oui	Oui
NetQoS NQMySql (nfa_mysqlCSE sous Linux)	Oui	Oui	Oui	Oui
Gestionnaire de NetQoS Reporter	Oui		Oui	
Services généraux de NetQoS Reporter/Analyzer	Oui		Oui	

Service	Autonome	Harvester	Console	DSA (3 niveaux)
Service de pompage NetQoS Reporter/Analyzer	Oui		Oui	
Services de requête NetQoS Reporter/Analyzer	Oui		Oui	
Rapport de NetQoS Reporter/Analyzer	Oui		Oui	
Outil de surveillance de NetQoS Reporter/Analyzer	Oui		Oui	

Désinstallation du logiciel

Cette rubrique décrit la procédure de désinstallation du logiciel CA Network Flow Analysis à l'aide du programme de désinstallation. Vous pouvez désinstaller également le logiciel à partir de la fenêtre Ajout ou suppression de programmes de Windows. Le logiciel apparaît sous l'éditeur CA Technologies, Inc.

Remarque : Les étapes de cette rubrique supposent que vous désinstallez le logiciel CA Network Flow Analysis à partir d'un serveur de déploiement autonome ou distribué sur lequel aucun autre logiciel lié n'est installé.

Procédez comme suit :

1. Connectez-vous en tant qu'utilisateur possédant des droits d'administration au niveau de CA Network Flow Analysis.
2. Sauvegardez les données et les fichiers de configuration. Pour plus d'informations sur cette étape, reportez-vous au *Manuel de l'administrateur de CA Network Flow Analysis*.
3. Fermez toutes les applications (sans exceptions).
4. Lancez le programme de désinstallation : double-cliquez sur le raccourci du programme de désinstallation dans <chemin_installation>\Uninstall :
   - Système autonome : double-cliquez sur le raccourci Uninstall Reporter (Désinstaller le Reporter) pour désinstaller la console NFA en premier, puis double-cliquez sur le raccourci Uninstall Harvester (Désinstaller le Harvester) pour désinstaller le Harvester.

     Si vous essayez de désinstaller le logiciel du Harvester en premier, un message d'erreur s'ouvre.
   - Déploiement distribué : double-cliquez sur Désinstaller Reporter (serveur de console NFA), Désinstaller Harvester (serveur de Harvester) ou Désinstaller DSA (serveur de DSA).

   La fenêtre de désinstallation s'ouvre.

5. Cliquez sur **Désinstaller**.

   La désinstallation supprime tous les fichiers de programme et de données, y compris les éléments CA Network Flow Analysis et MySQL suivants :

   - Data (Données)
   - Services
   - Entrées du Registre
   - Raccourcis, liens et alias
   - La plupart des fichiers
   - Certains répertoires

   Une fois le processus terminé, la fenêtre affiche une liste des répertoires et des fichiers qui n'ont pas été supprimés.

   Remarque : N'utilisez pas le système de fichiers tant que la désinstallation est en cours. N'essayez pas d'afficher la progression dans l'explorateur Windows, par exemple.

   Une fois que le programme se termine, la fenêtre Fin de la désinstallation s'ouvre.

6. Pour fermer la fenêtre Fin de la désinstallation, cliquez sur **Terminé**.

7. Patientez quelques minutes pour permettre au processus d'aide de terminer le dernier nettoyage.

   Certains fichiers ne seront supprimés qu'à l'issue de cette phase. Une fois le dernier nettoyage terminé, le programme de désinstallation est également supprimé.

8. Consultez les informations suivantes pour vérifier que la désinstallation a fonctionné :

   a. Vérifiez que les clés de registre ont été supprimées dans l'emplacement suivant :

      HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\NetQoS

   b. Vérifiez que les services CA Network Flow Analysis ont été supprimés.

   c. Vérifiez que les programmes CA Network Flow Analysis (NFA, Harvester et MySQL par exemple) ne sont plus visibles dans le Panneau de configuration. S'ils le sont encore, sélectionnez chaque programme individuellement et cliquez sur **Désinstaller**.

Remarques :

- Le journal de désinstallation se trouve à la racine de l'emplacement d'installation d'origine. Par exemple, le journal de désinstallation du Harvester se trouve à l'emplacement suivant : <chemin_installation>\Harvester_Uninstall_<horodatage>.txt.
- Vous pouvez supprimer manuellement tous les répertoires et les fichiers CA Network Flow Analysis qui sont encore présents.
- Si la réinstallation du logiciel échoue, contactez le service du support de CA.

Chapitre 9: Dépannage

Cette section fournit des conseils de dépannage pour les problèmes détectés par les tests des éléments requis. Les tests des éléments requis peuvent générer des avertissements ou des messages d'erreur. Si un avertissement s'affiche, vous pouvez corriger le problème immédiatement ou après l'exécution du logiciel d'installation ou de mise à niveau. Vous devez corriger le problème pour pouvoir poursuivre. La plupart des rubriques de dépannage concernent des erreurs relatives aux éléments requis.

Remarque : De nombreux tests des éléments requis utilisent des indicateurs généraux pour l'identification des problèmes. La réussite d'un test des éléments requis ne garantit pas une configuration correcte. Il est important de respecter toutes les exigences et de terminer les tâches de configuration décrites dans ce manuel.

Les tests nécessaires suivants doivent être exécutés :

Test	Description	Avertissement ou échec	Serveur
Navigateur	Vérifie le registre d'un navigateur. Vérifiez qu'une version de navigateur prise en charge est installée (page 23).	Warning (Avertissement)	Autonome ou de console NFA
DEP	Vérifie que le service winmgt est en cours d'exécution. Configurez DEP suivant les instructions contenues dans ce manuel. (page 33)	Warning (Avertissement)	Serveurs Windows
Stratégie d'algorithme FIPS	Vérifie que la stratégie d'algorithme FIPS n'est pas activée (page 82).	Vérification du correctif automatique ou erreur	Autonome ou de console NFA
IIS installé	Vérifie que le service wcsvc est en cours d'exécution. Installez et configurez IIS en suivant les instructions contenues dans ce manuel (page 28).	Warning (Avertissement)	Autonome ou de console NFA
IIS Version (Version SAML)	Recherche IIS version 7.0 dans le Registre.	Warning (Avertissement)	Autonome ou de console NFA
Version .NET 3.5	Recherche .NET version 3.5 SP1. Si la version 3.5 est détectée, le Service Pack 1 est activé.	Erreur	Autonome ou de console NFA
Installation de NPC détectée	Vérifie si NPC est installé sur le serveur (page 83).	Erreur	Autonome ou de console NFA

Test	Description	Avertissement ou échec	Serveur
Commande de contrôle des services	Vérifie que le répertoire Windows System32 contient le fichier sc.exe (page 83).	Erreur	Serveurs Windows
SNMP	Vérifie que le service snmp s'exécute et que l'ID de processus est présent. Configurez SNMP sur des serveurs Windows (page 30) et des serveurs Linux (page 38).	Warning (Avertissement)	Tous les serveurs
Détection de Windows 2003	Vérifie que le serveur exécute Windows Server 2008, et non Windows Server 2003 (page 85).	Erreur	Serveurs Windows

Ce chapitre traite des sujets suivants :

Stratégie d'algorithme FIPS activée

Valide sur la console uniquement

Lorsque vous cliquez sur Suivant dans la fenêtre Contrat de licence dans le programme d'installation ou de mise à niveau de la console NFA, un message Avertissement de vérification des éléments requis s'ouvre, incluant le texte suivant :

> La clé de registre FipsAlgorithmPolicy de ce système a été activée. Si la clé suivante est également activée, Windows n'autorisera pas l'exécution de certains algorithmes.

Le message d'erreur apparaît, car une vérification de système a trouvé la clé FipsAlgorithmPolicy dans le Registre Windows, indiquant que la norme cryptographique FIPS (Federal Information Processing Standard) 140 est activée. Lorsque que cette stratégie est activée, le serveur peut exécuter uniquement les algorithmes cryptographiques qui ont été soumis au National Institute of Standards and Technology (NIST) et approuvés.

Cette restriction peut créer des problèmes de connexion aux bases de données via Open Database Connectivity (ODBC). Des problèmes de connectivité avec CA Network Flow Analysis peuvent survenir.

Pour désactiver la clé de registre FipsAlgorithmPolicy, cliquez sur OK dans le message Avertissement de vérification des éléments requis. La stratégie d'algorithme FIPS est désactivée et ne limite pas les connexions à la base de données.

Installation de NPC détectée

Valide sur la console

Si vous essayez de lancer le programme d'installation ou de mise à niveau sur un serveur doté de NetQoS Performance Center, un message d'erreur s'affiche et l'installation est annulée.

Vous ne pouvez pas installer CA Network Flow Analysis sur le même serveur que CA NetQoS Performance Center. Vous devez désinstaller complètement NPC pour pouvoir continuer l'installation ou la mise à niveau de CA Network Flow Analysis.

SC.exe non installé

Valide sur la console, le Harvester ou le DSA

Lorsque vous cliquez sur Suivant dans la fenêtre Contrat de licence du programme d'installation ou de mise à niveau, un message d'erreur commençant par le texte suivant s'ouvre :

> sc.exe n'est pas installé. Le programme d'installation n'a pas trouvé "sc.exe" dans le dossier System32.

Suite à la vérification du système, la commande de contrôle des services (fichier sc.exe) est introuvable dans le répertoire Windows/System32. La commande de contrôle des services est utilisée pour communiquer avec le contrôleur de services lors des opérations de ligne de commande. Si un fichier est manquant, le programme d'installation ou de mise à niveau se ferme.

Le fichier sc.exe est inclus dans le logiciel de Windows Server par défaut. Pour corriger le problème, restaurez le fichier sc.exe manquant à partir du logiciel d'installation de Windows Server, du Kit de ressources techniques Windows ou autre ressource.

Protocole SNMP non activé

Lorsque vous cliquez sur Suivant dans la fenêtre Contrat de licence du programme d'installation ou de mise à niveau, un message d'avertissement SNMP s'ouvre. Contenu du message :

> Avertissement de vérification des éléments requis. Les problèmes suivants ont été détectés : Le protocole SNMP n'est pas activé. Bien qu'elles ne soient pas requises avant l'installation, certaines fonctionnalités peuvent ne pas fonctionner correctement si ces problèmes ne sont pas résolus.

Le message d'avertissement SNMP apparaît lorsque la vérification des éléments requis ne détecte pas l'exécution du démon snmpd. Vous pouvez corriger le problème lorsque l'avertissement s'affiche ou procéder à l'installation ou à la mise à niveau. Cependant, pour que CA Network Flow Analysis s'exécute correctement, vous devez configurer le protocole SNMP (page 38) et vous assurer que les démons snmpd et snmptrapd s'exécutent.

Utilisez les procédures suivantes pour vérifier le statut SNMP sur un serveur Linux.

Procédez comme suit :

1. (Facultatif) Dans une fenêtre de terminal, entrez la commande de statut :
   `/etc/init.d/snmpd status`

   La commande renvoie l'ID de processus du démon snmpd. Si le texte de retour ne contient pas d'ID de processus pour le démon snmpd, celui-ci ne s'exécute pas.

2. (Facultatif) Vérifiez le statut dans la fenêtre Service Configuration :

   a. Ouvrez la fenêtre Service Configuration : sélectionnez System, Administration, Server Settings, Services.

      La fenêtre Service Configuration s'ouvre et l'onglet Background Services est sélectionné.

   b. Localisez snmpd et snmptrapd dans la liste des services.

   c. Vérifiez le statut de ces services :

      - Sélectionnez snmpd et révisez le message de statut qui est affiché.
      - Sélectionnez snmptrapd et révisez le message de statut qui est affiché.

   d. Fermez la fenêtre Service Configuration.

Windows Server 2003 détecté

Un message d'erreur s'affiche si vous essayez de lancer le programme d'installation ou de mise à niveau sur un serveur qui exécute Windows Server 2003. L'installation et la mise à niveau sur des serveurs Windows sont prises en charge uniquement pour les serveurs qui exécutent Windows Server 2008 R2, Standard Edition.

Procédez à la mise à niveau vers Windows Server 2008 R2 Standard Edition avant de poursuivre l'installation ou la mise à niveau.